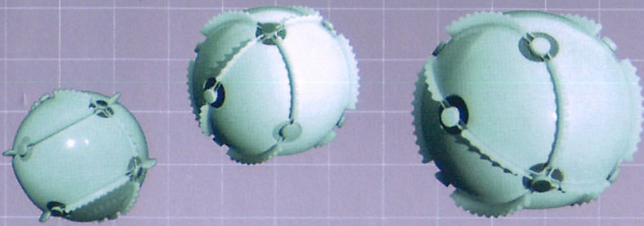
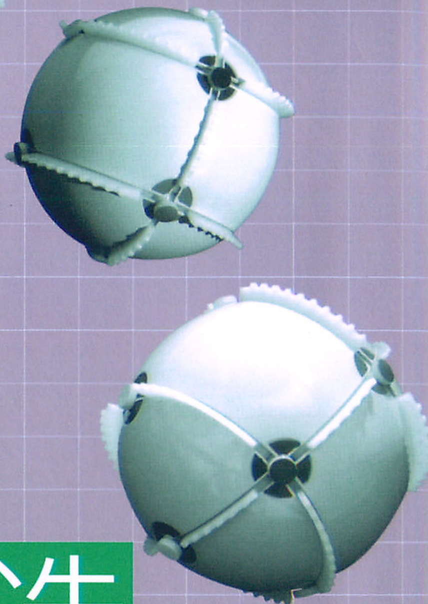
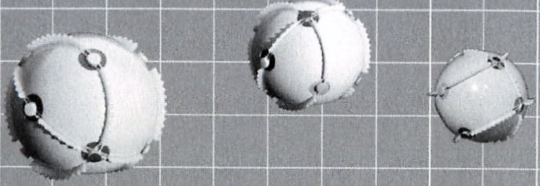


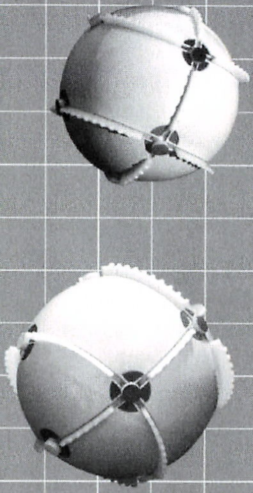


置換群から学ぶ組合せ構造

芳沢光雄

日本評論社





置換群から学ぶ組合せ構造

芳沢光雄

日本評論社

まえがき

3次，4次の方程式の解法は16世紀にイタリアで発見された．そして18世紀後半に，ラグランジュは5次方程式の解法を模索する過程で，3次方程式，4次方程式が解くことができる理論的な背景を研究し，根の置換という考え方が芽生えた．19世紀に入ってガロアは，任意の方程式にその根の集合上の置換群が対応し，それが方程式のべき根による可解性を決定していることを発見した．そのように，18世紀から19世紀前半が置換群，そして群の起源となるだろう．

現在，群論は，数学の他分野はもとより，量子力学のような自然科学ばかりでなく比較言語学のような人文科学の研究に至るまで様々なところに登場している．また，グラフ，デザイン，符号等の組合せ構造のうち，とくに対称性の強いものには自己同型群として深く関わっている．したがって，そこには置換群から組合せ構造を学ぶ一つの流れが存在する．ところが，諸分野が細分化してきたこと，あるいは有限単純群分類の完成のような特殊事情も加わって，その流れはあまり注目されていない．しかし，以下述べることなどを踏まえると，その流れをなるべく平易に説明する書がいろいろあってもよいと考えている．

筆者は10年前から日本の数学教育の形骸化が想像以上に進んでいることに危機感を抱き，その流れに歯止めをかけるための様々な活動を続けてきた．最近では文部科学省の企画のものであるなしに関わらず，日常生活と結びついた楽しい話題の授業を子供達に行うことに力を入れている．そのような活動を通して学んだことはたくさんあるが，次の二点をここで強調したい．一つは，背景や周囲との結びつきを説明しないで突然出てくる項目に対しては，子供達の違和感は強く，学ぶ意欲も低い．たとえば，1次変換のない2行2列の行列．もう一つは，長く続く議論の末に出てくることがらは，旅行ガイド書の写真のように，事前に目標とする結果とその応用を簡単に示した方が理解しやすい．たとえば，極限の概念を長く説明してから出てくる微積分の公式はそうである．

上記の観点からここ数年，置換群に関する話題で気になっていたことがいく

つかあった．前者との関連の例を挙げると，符号理論におけるゴレイ符号を説明するとき，ゴレイ符号を定義する大きな行列を突然与えて終りにするのではなく，マシュー群(3 章参照)やウィットシステム(4 章参照)との関連から説明したほうが良いこと．後者との関連の例も挙げると，長く続く拡大体の詳しい議論の後でようやく多項式のガロア群を登場させるのではなく，先に多項式から置換群的に派生するある多項式の既約分解によってその式のガロア群を導入し，目標の一部を見せてから拡大体の詳しい議論を行った方が良いと思ったこと．

そのような背景があって本書の執筆を始めたので，当初，符号理論やガロア群についても含める予定であった．しかし本書の目次にある項目の他に符号やガロア群を含めると少し重い本になってしまうこと，さらにそれらの本質はむしろ「体」にあるので別の書として丁寧に扱うのがよいと考えたこと，などから本書の目次に示した構成を決定した．

本書を読む上で必要な予備知識は，線形代数学の基本的なこと，および集合・写像に関するごく基本的な用語だけである．群，環，体については，初学者でも困らないように定義から説明した．

最後に，本書の原稿は諏訪東京理科大学の飯田洋市氏に一通り読んでいただき，いくつもの助言をいただいた．また日本評論社の佐藤大器氏には，企画段階から出版まで終始お世話になった．ここに合わせて，深く謝意を表する．

2004 年 10 月

芳沢 光雄

置換群から学ぶ組合せ構造 ●—● 目次

まえがき……i

記法……vi

1章

群の導入とその周辺

1

1.1 あみだくじと対称群……1
1.2 群の導入……5
1.3 剰余類……12
1.4 正規部分群と剰余群……15
1.5 準同型……19
1.6 直積と半直積……24
1.7 p-群……28
1.8 有限体……33
1.9 直交ラテン方陣……40

2章

多重可移置換群と組合せゲーム

45

2.1 置換群に関するいくつかの言葉……45
2.2 多重可移置換群……49
2.3 15ゲームと新15ゲーム……52
2.4 球面上のあるゲーム……56

3章

射影線形群とマシュー群

3.1 射影線形群 ……65
3.2 射影線形群の置換表現 ……67
3.3 可移拡大と可移置換群のランク ……70
3.4 マシュー群の構成 ……73
3.5 多重可移置換群の単純性 ……79
3.6 マシュー群のデザイン論的性質 ……82
65

4章

群とデザイン

4.1 デザイン ……87
4.2 対称的デザイン ……95
4.3 タイトデザイン ……101
4.4 デザインの軌道行列 ……109
4.5 アソシエーションスキームとウィットシステム ……111
87

5章 群とグラフ

121

5.1 グラフ……121
5.2 グラフの自己同型群として表現する群……128
5.3 グラフの固有値……134
5.4 距離正則グラフ……142

Appendix
無限次数多重可移置換群……151

参考文献……156

索引……160

記法

最初に，参考文献の［和；　］，［洋；　］，［論；　］は，順に和書，洋書，論文を表すことにする．

本書での記法の多くはなるべく標準的なものを用いるが，線形代数学や一般集合論でのごく基礎的なものについては［和；5］，［和；6］，［和；12］等を参照されたい．群論や組合せ論での記法はいくつかの点で他分野とやや異なるものがあり，組合せ記号の C はそれほど一般的でないことから，また集合の包含記号の意味は書によって若干の違いがあるので，そのような点を含めて本書を読む上で注意が必要と思われる記法を以下まとめて述べよう．

$\boldsymbol{N}, \boldsymbol{Z}, \boldsymbol{Q}, \boldsymbol{R}, \boldsymbol{C}$ を順に，自然数，整数，有理数，実数，複素数全体からなる集合とする．それらは，和や積などの演算を定めて扱うことが多い．

集合 A が集合 B の部分集合であることを

$$A \subseteqq B \quad \text{あるいは} \quad B \supseteqq A$$

で表し，とくに A が B の真部分集合であることを

$$A \subsetneqq B \quad \text{あるいは} \quad B \supsetneqq A$$

で表す．また，空集合を $\emptyset$ で表す．集合 A が有限集合で，その元(要素)の個数が n のとき $|A| = n$ で表し，集合 A が無限集合のとき $|A| = \infty$ で表す．なお，集合の元(要素)を点ということもある．

集合 S が互いに素な部分集合 $T_i\ (i \in I)$ の直和になっているとき，

$$S = \sum_{i \in I} T_i$$

と書く．とくに，I が有限集合 $\{1, 2, \cdots, n\}$ であるとき，

$$S = T_1 + T_2 + \cdots + T_n$$

と書く．

命題 P が成立すれば命題 Q も成立することを

$$P \Longrightarrow Q$$

で表す．そして，命題 P と命題 Q が同値であることを

$$P \Longleftrightarrow Q$$

で表す．

相違なる n 個のものから r 個を選ぶ場合の数を高校の教科書では

$${}_n\mathrm{C}_r$$

によって表すが，本書では国際的に広く用いられている

$$\binom{n}{r}$$

によって表す．

集合 A から集合 B への写像 f と集合 B から集合 C への写像 g が与えられているとき，f と g の合成写像を本書では

$$f \circ g \quad \text{あるいは} \quad fg$$

によって表す．そして，A の元 a の f による像を

$$(a)f \quad \text{あるいは} \quad a^f$$

によって表す．このように定めることによって，指数法則から連想できる

$$a^{fg} = (a^f)^g$$

が成り立つ．また，A の部分集合 $\varDelta$ に対し，B の部分集合 $\{(a)f \mid a \in \varDelta\}$ を

$$(\varDelta)f \quad \text{あるいは} \quad \varDelta^f$$

によって表す．

最後に，2 つの整数 a と b に対し，a が b の約数であることを $a|b$ で表し，a と b の最大公約数を (a, b) で表す．また，$a-b$ が自然数(正の整数) n の倍数のとき，

$$a \equiv b \qquad (\bmod n)$$

で表し，a と b は n を法として**合同**であるという．

1章 群の導入とその周辺

1.1 あみだくじと対称群

今日の日本では，たてに引いた何本かの平行線の間に横線をあちこちに入れて行うあみだくじは広く行われており，日本の誇れる文化の一つになった感がある．あみだくじは江戸末期の頃から流行し始めたが，当時は何本かの直線を放射線状に書いて，それらの末端の中心部に金額や役を書いて隠しておき，それらの先端を指名させていた(日本大百科全書，大日本百科事典(小学館)などを参照)．

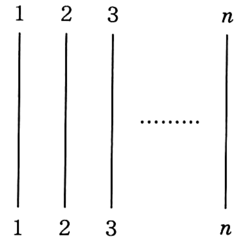
本書ではあみだくじから対称群を導入しよう．最初に，写像に関するいくつかの言葉を復習する．

f を集合 A から集合 B への写像とする．f が(A から B への)**単射**であるとは，A の相異なる任意の 2 元 a, a' に対し $(a)f \neq (a')f$ となることである．f が(A から B への)**全射**であるとは，B の任意の元 b に対し $(a)f = b$ となる A の元 a が存在することである．そして f が単射かつ全射であるとき，f は(A から B への)**全単射**であるという．

f が A から B への全単射であるとき，B の任意の元 x に対し $(y)f = x$ となる A の元 y を対応させる規則によって，B から A への写像が定義される．この写像を f の**逆写像**といい，f^{-1} によって表す．明らかに，f^{-1} は(B から A への)全単射である．とくに，集合 Ω から Ω 自身への全単射を Ω 上の**置換**という．

定理 1.1.1

n 本のたて線が引かれているあみだくじの原形があり，その上部と下部両方に左から $1, 2, \cdots, n$ が振ってあるとする．このとき $\{1, 2, \cdots, n\}$ 上の任意の置換 σ に対し，何本かの適当な横線を引いて σ と同じ作用をするあみだくじを作る



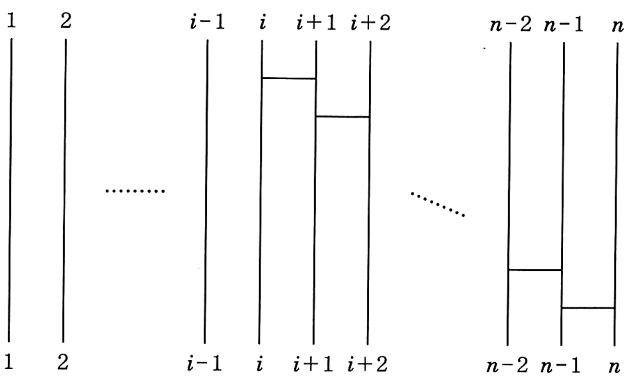
ことができる.

証明

n に関する数学的帰納法で示す.

$n=1$ のとき，たて線が 1 本だけなので明らかに成立する.

$n-1$ まで成り立つと仮定する．もし $(n)\sigma=n$ ならば，仮定を用いて，右端のたて線を除く $n-1$ 本のたて線の間に横線を何本か引くことによって σ と同じ作用をするあみだくじを作ることができる．もし $(n)\sigma\neq n$ で $(i)\sigma=n$ $(i\neq n)$ とすると，図のようにあみだくじの上部に次の部分を付けることを考えると，初めに i が n にたどり着くことができる.



よって σ と同じ作用をするあみだくじの構成を考えると，残りは右端のたて線を除く $n-1$ 本のたて線の間に横線を何本か引くことによって作ればよいが，これは数学的帰納法の仮定によってできる.

したがって，n のときも成立する．

有限集合 Ω 上の任意の置換 f, g に対し，$f\circ g$ も Ω 上の置換となる．すなわち，Ω 上の置換全体からなる集合 S^{Ω} においては，写像の合成に関する演算 $\circ$ が定義できる．その演算を定めた S^{Ω} を Ω 上の**対称群**といい，$|\Omega| = n$ のとき S^{Ω} を S_n と書いて n 次対称群という．

S^{Ω} は演算 $\circ$ に関して結合法則

$$(f\circ g)\circ h = f\circ (g\circ h)$$

が一般に成り立ち，Ω 上の恒等写像 e を元としてもつ．さらに，S^{Ω} の任意の元 f に対し，f の逆写像 f^{-1} も S^{Ω} の元である．

定理 1.1.1 でのあみだくじについて述べると，$\Omega = \{1, 2, \cdots, n\}$ 上の任意の置換 f, g に対し，f と同じ作用をするあみだくじの下に g と同じ作用をするあみだくじを付けると，その合わせたあみだくじは $f\circ g$ と同じ作用をするあみだくじになる．また，横線が 1 本も引かれていないあみだくじは e と同じ作用をする．さらに，Ω 上の任意の置換 f に対し，f と同じ作用をするあみだくじのたどる順序を逆に下から上にして考えると，それは f^{-1} と同じ作用をするあみだくじになる．

有限集合 Ω の相異なる t 個の元 $\alpha_1, \alpha_2, \cdots, \alpha_t$ に対し，α_i を α_{i+1} $(i = 1, 2, \cdots, t-1)$，α_t を α_1 に移し，それら以外の Ω の元を固定する Ω 上の置換を

$$(\alpha_1 \quad \alpha_2 \quad \cdots \quad \alpha_t) \quad \text{または} \quad (\alpha_1, \alpha_2, \cdots, \alpha_t)$$

で表し，そのようなものを一般に長さ t の**巡回置換**という．とくに，長さ 2 の巡回置換を**互換**という．

定理 1.1.1 から次の定理は直ちに導かれる．

定　理 | 1.1.2

$\Omega = \{1, 2, \cdots, n\}$ 上の対称群 S_n の任意の元は，次の互換いくつかの重複を含めた合成によって表される．

$$(1 \quad 2),\ (2 \quad 3),\ (3 \quad 4),\ \cdots,\ (n-1 \quad n)$$

ここで問題となるのは，定理 1.1.2 で述べた表示についてはどのようにして得るのか，ということである．そこで，Ω 上の任意の置換 σ に対して

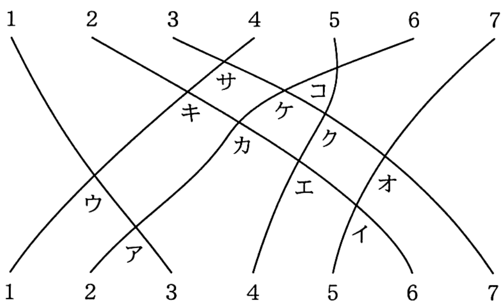
$$\sigma = \begin{pmatrix} 1 & 2 & \cdots\cdots & n \\ (1)\sigma & (2)\sigma & & (n)\sigma \end{pmatrix}$$

という記法を定めて，次の $n=7$ の場合の例で紹介しよう．なお，それを一般の n に拡張できることは容易に納得できるだろう．

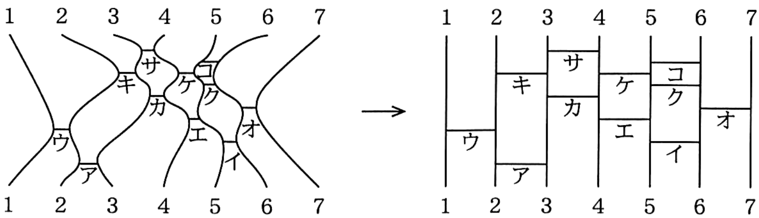
例 1.1.3

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 6 & 7 & 1 & 4 & 2 & 5 \end{pmatrix}$$

とする．最初に，1 が 3，2 が 6，3 が 7，4 が 1，5 が 4，6 が 2，7 が 5 にたどり着くあみだくじを次のように構成する．



上図は σ に対応する 7 本の線を引いたものであるが，線は上から下に向かい，途中で曲がっても構わないものの，線どうしは接することがなく，また 3 本以上の線が同じ点で交わることはないようにする．次に，交点ア，イ，ウ，エ，オ，カ，キ，ク，ケ，コ，サをそれぞれあみだくじの横線に見立てて σ と



同じ作用をするあみだくじを作る．

以上から次式を得る．なお，たとえば(サ)と(カ)は互換(3　4)を表しており，本書では，写像の演算は左から行っていることに注意する．

$$\sigma = (サ)(コ)(ケ)(ク)(キ)(カ)(オ)(エ)(ウ)(イ)(ア)$$
$$= (3\quad 4)(5\quad 6)(4\quad 5)(5\quad 6)(2\quad 3)(3\quad 4)(6\quad 7)(4\quad 5)(1\quad 2)(5\quad 6)(2\quad 3)$$

1.2　群の導入

集合 G に演算 $*$ が定義されているとき，すなわち任意の $a, b \in G$ に対して $a*b \in G$ が成り立つとき，次の条件(1)，(2)，(3)をみたすならば G は $*$ に関して**群**であるという．なお，とくに演算記号を意識する必要がない場合，$a*b$ を単に ab で表すことが普通である．また，演算記号として・を用いることもよくある．

(1)　**結合法則**が成り立つ．すなわち，任意の $a, b, c \in G$ に対して

$$(a*b)*c = a*(b*c)$$

が成り立つ．

(2)　**単位元**をもつ．すなわち，ある元 $e \in G$ があって，G の任意の元 a に対して

$$a*e = e*a = a$$

が成り立つ．e を G の単位元というが，本書では普通 1 で表す．

(3)　すべての元は**逆元**をもつ．すなわち，任意の元 $a \in G$ に対して，

$$a*b = b*a = e \quad (単位元)$$

となる $b \in G$ がある．b を a の逆元とよび，普通 a^{-1} で表す．

また，(1)，(2)，(3)の他に**交換法則**

(4)　G の任意の元 a, b に対して

$$a*b = b*a \qquad (a と b は\textbf{可換})$$

が成り立つとき，G を**可換群**または**アーベル群**という．可換群 G の演算は $+$ で表すこともあり，その場合 $a+b$ を a と b の**和**といい，G を**加法群**という．そして，加法群 G の単位元はとくに**零元**といい，それを 0 で表す．さらに，b

の逆元を $-b$ で表し，$a+(-b)$ を $a-b$ で表す.

演算 $*$ が定義されている群 G において，単位元は唯一である．実際，1 と $1'$ を単位元とすると，

$$1 = 1 * 1' = 1'$$

となる．そして任意の元 x に対して，その逆元も唯一である．実際，y と y' を x の逆元とすると，

$$y = y * (x * y') = (y * x) * y' = y'$$

となる．なお上の議論から，群の定義の(2)と(3)は，それぞれ一方の演算式だけでもよいことを意味している.

例 | 1.2.1

（ア） 有限集合 Ω 上の対称群 S^{Ω} は写像の合成 $\circ$ に関して群である.

（イ） 整数全体の集合 $\boldsymbol{Z}$ は和 $+$ に関して加法群であるが，自然数全体の集合 $\boldsymbol{N}$ は $+$ に関して群ではない.

（ウ） 実数全体の集合 $\boldsymbol{R}$ から 0 を除いた集合 $\boldsymbol{R}^* = \boldsymbol{R} - \{0\}$ は積・に関して可換群であるが，$\boldsymbol{R}$ は・に関して群ではない.

1.1 節において有限集合上の任意の置換はいくつかの互換の合成として表されることを示したが，一般に次のことが成り立つ.

定　理 | 1.2.2

有限集合 Ω 上の任意の置換 σ を互換の合成として表すとき，その個数 r が偶数であるか奇数であるかは σ によって一意的に定まる.

証　明 ……W. I. Miller［論；25］参照

いま，$\Omega = \{1, 2, \cdots, n\}$ とおき，σ が

$$\sigma = (\alpha_1 \quad \beta_1)(\alpha_2 \quad \beta_2) \cdots (\alpha_r \quad \beta_r) = (\gamma_1 \quad \delta_1)(\gamma_2 \quad \delta_2) \cdots (\gamma_s \quad \delta_s)$$

と 2 通りに表されたとする．このとき

$$(\alpha_r \quad \beta_r)\cdots(\alpha_2 \quad \beta_2)(\alpha_1 \quad \beta_1)(\gamma_1 \quad \delta_1)(\gamma_2 \quad \delta_2)\cdots(\gamma_s \quad \delta_s)$$
$$= e \quad (\text{恒等写像})$$

となるので，$r+s$ が偶数であることを示せば r と s の偶奇性は一致する．

そこで，e がいくつかの互換 $k_1, k_2, \cdots, k_r$ の合成として

$$e = k_1 \circ k_2 \circ \cdots \circ k_r \tag{1}$$

と表されたとするとき，r は偶数になることを示せばよい．まず，Ω の元 1 が現れる k_i があるとし，それらのうちで i が最大となるものを改めて $k_i = (1 \quad \alpha)$ (α は 1 と異なる Ω の元) とする．ここで $i \neq 1$ である．なぜならば，もし $i=1$ とすると，(1)式の右辺は e と異なるものになるからである．そして，k_{i-1} は次の 4 通りのどれかになる．

（ア）　$(1 \quad \alpha)$

（イ）　$(1 \quad \beta)$　　(β は 1，α と異なる Ω の元)

（ウ）　$(\alpha \quad \beta)$　　(β は 1，α と異なる Ω の元)

（エ）　$(\beta \quad \gamma)$　　($\{\beta, \gamma\} \cap \{1, \alpha\} = \emptyset$)

それぞれの場合に対して，以下の等式が成り立つ．

（ア）　$k_{i-1} \circ k_i = e$

（イ）　$k_{i-1} \circ k_i = (1 \quad \beta) \circ (1 \quad \alpha) = (1 \quad \beta \quad \alpha) = (1 \quad \alpha) \circ (\alpha \quad \beta)$

（ウ）　$k_{i-1} \circ k_i = (\alpha \quad \beta) \circ (1 \quad \alpha) = (1 \quad \alpha \quad \beta) = (1 \quad \beta) \circ (\alpha \quad \beta)$

（エ）　$k_{i-1} \circ k_i = (\beta \quad \gamma) \circ (1 \quad \alpha) = (1 \quad \alpha) \circ (\beta \quad \gamma)$

そこで，(1)式の右辺の $k_{i-1} \circ k_i$ に上の等式を代入したものを

$$e = h_1 \circ h_2 \circ \cdots \circ h_s \tag{2}$$

とすれば，(2)式の右辺の互換の個数 s は $r-2$ または r と等しく，さらに Ω の元 1 が現れる h_j に対しては，$j \leqq i-1$ が成り立つ．

次に，(2)式に対しても(1)式に対する議論と同じことを行い，さらにその議論をくり返し行うと，

$$e = q_1 \circ q_2 \circ \cdots \circ q_t \tag{3}$$

を得る．ここで，すべての互換 q_i に Ω の元 1 は現れず，t と r の偶奇性は一致する．

さて，Ω の元 1 に対する議論は Ω の元 2，3，4，… にもそれぞれ適用できる

ので，(3)式に対し順次適用していけば，いずれ右辺は e になる．したがって，t は偶数であることが分かる．よって r は偶数である．

定理 1.2.2 において，r が偶数のとき σ を**偶置換**といい，r が奇数のとき σ を**奇置換**という．

有限集合 Ω 上の任意の偶置換 f, g に対し，$f \circ g$ も Ω 上の偶置換となる．すなわち，Ω 上の偶置換全体からなる集合 A^Ω には写像の合成の演算 $\circ$ が定義できる．その演算を定めた A^Ω を Ω 上の**交代群**といい，$|\Omega| = n$ のとき A^Ω を A_n と書いて n 次交代群という．

A^Ω は S^Ω の部分集合であるから，A^Ω は演算 $\circ$ に関して結合法則が成り立つ．また，Ω 上の恒等写像 e は偶置換である．さらに，

$$(\alpha_1 \quad \beta_1)(\alpha_2 \quad \beta_2)\cdots(\alpha_{2t-1} \quad \beta_{2t-1})(\alpha_{2t} \quad \beta_{2t})$$

に対して，

$$(\alpha_{2t} \quad \beta_{2t})(\alpha_{2t-1} \quad \beta_{2t-1})\cdots(\alpha_2 \quad \beta_2)(\alpha_1 \quad \beta_1)$$

はその逆写像である．したがって A^Ω も S^Ω と同様に，写像の合成 $\circ$ に関して群となる．

群 G において，G の元の個数 $|G|$ を G の**位数**という．位数が有限の群を**有限群**といい，無限の群を**無限群**という．

例 1.2.3

無限集合 Ω に対し，

$$S^\Omega = \{g \mid g \text{ は } \Omega \text{ 上の置換}\}$$
$$FS^\Omega = \{g \mid g \text{ は } \Omega \text{ 上の置換}, \ |\{\omega \in \Omega \mid (\omega)g \neq \omega\}| < \infty\}$$
$$A^\Omega = \{g \in FS^\Omega \mid \{\omega \in \Omega \mid (\omega)g \neq \omega\} \text{ 上 } g \text{ は偶置換}\}$$

とおくと，それらは写像の合成 $\circ$ に関して無限群である．S^Ω を Ω 上の対称群，FS^Ω を Ω 上の**有限的対称群**，A^Ω を Ω 上の交代群という．

群 G の空でない部分集合 H が G と同じ演算に関して群となるとき H を G

の**部分群**といい，$H \leqq G$ で表す．さらに $H \neq G$ であるとき，H を G の**真部分群**といい，$H < G$ で表す．G 自身および単位元のみからなる部分群 $\{1\}$ は明らかに G の部分群であり，それらを G の**自明な部分群**という．ここで $\{1\}$ を**単位群**といい，それを単に 1 と書くことが多い．H_λ $(\lambda \in \Lambda)$ を G の部分群とすると（Λ はある集合），それらの共通集合 $\bigcap_{\lambda \in \Lambda} H_\lambda$ が G の部分群になることはやさしく分かる．

集合 Ω 上の対称群 S^Ω の部分群を Ω 上の**置換群**という．$|\Omega| = n$ のとき，G を**次数** n の置換群ともいう．

例 1.2.4

$\Omega = \{1,2,3,4\}$ のとき，$\{1,\ (1\ \ 2\ \ 3\ \ 4),\ (1\ \ 3)(2\ \ 4),\ (1\ \ 4\ \ 3\ \ 2)\}$ と $\{1,\ (1\ \ 2)(3\ \ 4),\ (1\ \ 3)(2\ \ 4),\ (1\ \ 4)(2\ \ 3)\}$ はともに位数 4 の Ω 上の置換群であり，$\{1,\ (1\ \ 2\ \ 3\ \ 4),\ (1\ \ 3)(2\ \ 4),\ (1\ \ 4\ \ 3\ \ 2),\ (1\ \ 3),\ (1\ \ 4)(2\ \ 3),\ (2\ \ 4),\ (1\ \ 2)(3\ \ 4)\}$ は位数 8 の Ω 上の置換群である．

群においては結合法則が成り立つので，演算の順序を変えても演算を行う元の並べ方を変えなければ演算結果は同一である．実際，群 G の元 $a_1, a_2, \cdots, a_m$ に対して，

$$(\cdots\cdots(((a_1a_2)a_3)a_4)\cdots a_m) = \cdots = (a_1\cdots(a_{m-3}(a_{m-2}(a_{m-1}a_m)))\cdots)$$

が成り立つ．それゆえ，上式に示された G のどの元も $a_1a_2\cdots a_m$ で表してよいのである．そして，G の元 x と自然数 n に対して，

$$x^n = \underbrace{xx\cdots x}_{n\text{個}}, \qquad x^{-n} = \underbrace{x^{-1}x^{-1}\cdots x^{-1}}_{n\text{個}}, \qquad x^0 = 1$$

と定める．これによって整数 r, s に対して，

$$x^{r+s} = x^r x^s, \qquad (x^r)^s = x^{rs}$$

が一般に成り立つ．

群 G の部分集合 S に対して，

$$\langle S \rangle = \{x_1^{r_1}x_2^{r_2}\cdots x_m^{r_m} \mid x_i \in S,\ \ r_i \text{ は整数}\}$$

とおくと，これは G の部分群になる．それを S で**生成**された G の部分群とい

い，S をその**生成系**という．S で生成された G の部分群は，S を含む G の部分群のうちで最小のものである．すなわち，

$$\langle S\rangle = \bigcap_{H:\,S\text{を含む}\,G\text{の部分群}} H$$

であることが容易に分かる．そして，上式を $\langle S\rangle$ の定義式とする書もある．なお $S=\{a_1, a_2, \cdots, a_n\}$ のとき，$\langle S\rangle$ を $\langle a_1, a_2, \cdots, a_n\rangle$ とも書く．とくに $S=\{a\}$ のとき，$\langle S\rangle=\langle a\rangle$ を a で生成される**巡回群**といい，a をその**生成元**という．明らかに

$$\langle a\rangle = \{a^m \mid m\in \boldsymbol{Z}\}$$

が成り立ち，その位数 $|\langle a\rangle|$ を a の位数といい，$|a|$ で表す．とくに $|a|=n<\infty$ のとき，

$$\langle a\rangle = \{1, a, a^2, \cdots, a^{n-1}\}$$

である．

例 1.2.5

$\Omega=\{1,2,\cdots,n\}$ のとき，

$$a=(1,2,\cdots,n),\qquad b=(1\quad 2)$$

とおくと，

$$S^{\Omega}=\langle a,b\rangle$$

が成り立つ．

証明

$$a^{-1}ba=(2\quad 3),\qquad a^{-2}ba^2=(3\quad 4),\qquad \cdots,$$
$$a^{-n+2}ba^{n-2}=(n-1\quad n)$$

であるから，

$$(1\quad 2),\ (2\quad 3),\ (3\quad 4),\ \cdots,\ (n-1\quad n)\in\langle a,b\rangle.$$

したがって，定理 1.1.2 を用いて

$$S^{\Omega}=\langle a,b\rangle$$

を得る．

定 理 | 1.2.6

位数 n の巡回群 $G=\langle a\rangle$ において，任意の部分群は巡回群となり，n の任意の約数 m に対して，位数 m の部分群はただ 1 つ存在する．

証 明

G の部分群 $H\neq 1$ に対して，$a^i\in H$ となる自然数 i のうちで最小のものを改めて i とおく．H の任意の元 a^j に対して，

$$j=ir+s \qquad (0\leqq s\leqq i-1)$$

となる整数 r,s をとると，

$$a^s=a^{j-ir}=a^j\cdot(a^i)^{-r}\in H$$

となる．ここで i の最小性を用いると，$s=0$ を得る．よって，$H=\langle a^i\rangle$ が成り立つ．

次に，$|a^{n/m}|=m$ であるので，G には位数 m の部分群が存在する．さらに K を位数 m の任意の部分群とし，$a^k\in K$ となる自然数 k のうちで最小のものを改めて k とおくと，j を i で割った余り s が 0 になった上の議論と同様に考えて，$K=\langle a^k\rangle$ および $k|n$ が分かる．したがって，

$$\frac{n}{k}=|K|=m$$

から $k=\dfrac{n}{m}$ が成り立つので，K の一意性が示された．

本節の最後に紹介する次の例は，**巡回置換分解**という言葉によって広く知られている．

例 | 1.2.7

σ を集合 Ω 上の置換とし，σ の S^Ω における位数 $|\sigma|$ は有限とする．このとき，σ は互いに共通な文字をもたないいくつかの巡回置換の合成として表すことができる．また，それらの巡回置換の長さ (>1) として現れる相異なる数全体は有限個で，それらを $n_1,n_2,\cdots,n_s$ とすると，

$$|\sigma| = n_1, n_2, \cdots, n_s \text{ の最小公倍数}$$

が成り立つ．

たとえば，$\Omega = \boldsymbol{N}$ 上の置換

$$\sigma = (1\quad 2)(3\quad 4\quad 5)(6\quad 7)(8\quad 9\quad 10)$$
$$\cdots(5n+1\quad 5n+2)(5n+3\quad 5n+4\quad 5n+5)\cdots$$

の位数は 6 で，s は 2 となり，n_1 と n_2 はそれぞれ 2 と 3 である．

1.3 剰余類

群 G の部分集合 S, T と群 G の元 a, b に対して，

$$ST = \{xy \mid x \in S,\ y \in T\}$$
$$S^{-1} = \{x^{-1} \mid x \in S\}$$
$$aS = \{ax \mid x \in S\}$$
$$Sb = \{xb \mid x \in S\}$$

とおく．明らかに

$$|S| = |aS| = |Sb|$$

が成り立つ．

群 G とその部分群 H に対して，G の元 a, b の間の関係 $\sim$ を

$$a \sim b \Longleftrightarrow ab^{-1} \in H$$

によって定める．

$$aa^{-1} = 1 \in H$$

および

$$(ab^{-1})^{-1} = ba^{-1}$$

が成り立ち，さらに

$$ab^{-1}, \qquad bc^{-1} \in H$$

のとき

$$ac^{-1} = (ab^{-1})(bc^{-1}) \in H$$

となるので，$\sim$ は G における同値関係である．G の $\sim$ による各同値類は Hg $(g \in G)$ という形で表され，それを G における H の**左剰余類**という．H の左剰余類全体からなる集合を $H\backslash G$ で表し，$H\backslash G$ の各元から 1 つずつ代表元を

取り出してできる集合を G における H の**左代表系**という．$\{x_\nu \mid \nu \in I\}$ を G における H の左代表系とすると，

$$G = \sum_{\nu \in I} Hx_\nu \qquad (\text{直和})$$

となる．

一方，G の元 a, b の間の関係 $\sim$ を

$$a \sim b \Longleftrightarrow a^{-1}b \in H$$

によって定めると，$\sim$ も G における同値関係となる．この場合，$\sim$ による各同値類は $gH\,(g \in G)$ という形で表され，それを G における H の**右剰余類**という．H の右剰余類全体からなる集合を G/H で表し，G における H の**右代表系**も左代表系と同じように定める．いま，

$$Ha = Hb \Longleftrightarrow a^{-1}H^{-1} = b^{-1}H^{-1} \Longleftrightarrow a^{-1}H = b^{-1}H$$

であるので，$\{x_\nu \mid \nu \in I\}$ が G における H の左代表系ならば $\{x_\nu^{-1} \mid \nu \in I\}$ は G における H の右代表系となる．したがって，このとき

$$G = \sum_{\nu \in I} x_\nu^{-1} H \qquad (\text{直和})$$

が成り立つ．以上から $|H \backslash G| = |G/H|$ を得るが，この値を G における H の**指数**といい，$|G : H|$ で表す．そして，次の定理を得る．

定 理 | 1.3.1 ……………… **ラグランジュの定理**

有限群 G とその部分群 H に対して，

$$|G| = |G : H| \cdot |H|$$

が成り立つ．とくに G の任意の元 a に対して，

$$|a| \,\Big|\, |G|, \qquad a^{|G|} = 1$$

が成り立つ．

集合 Ω 上の置換群 G と Ω の元 α に対して，

$$G_\alpha = \{g \in G \mid (\alpha)g = \alpha\}$$

とおくと，G_α は G の部分群となり，これを G における α の**固定部分群**とい

う．そして，

$$(\alpha)G = \{(\alpha)g \mid g \in G\}$$

とおくことにより，次の定理を得る．

定　理 | 1.3.2

有限集合 Ω 上の置換群 G と Ω の元 α に対して，

$$|G| = |(\alpha)G| \cdot |G_\alpha|$$

が成り立つ．

証　明

定理 1.3.1 より

$$|G| = |G : G_\alpha| \cdot |G_\alpha|$$

を得る．ここで，G の元 g, h に対して，

$$\begin{aligned}(\alpha)g = (\alpha)h &\Longleftrightarrow (\alpha)gh^{-1} = \alpha \\ &\Longleftrightarrow gh^{-1} \in G_\alpha \\ &\Longleftrightarrow G_\alpha g = G_\alpha h\end{aligned}$$

なので，

$$|(\alpha)G| = |G : G_\alpha|$$

が成り立ち，結論が得られる．

例 | 1.3.3

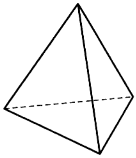
正多面体をそれ自身に移す合同変換全体は群になり，それを正多面体の**合同変換群**という．任意の正多面体に対してその頂点集合を Ω とすると，その合同変換群 G は Ω 上の置換群と見なすことができ，G は次の性質をもつ：Ω の任意の元 α, β に対して，$(\alpha)g = \beta$ となる $g \in G$ が存在する．

この性質および定理 1.3.2 を使うことによって，以下を得る．

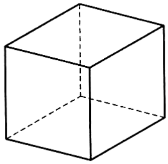
正 4 面体の合同変換群の位数			$= 4 \cdot 3 = 12$
正 6	〃	〃	$= 8 \cdot 3 = 24$
正 8	〃	〃	$= 6 \cdot 4 = 24$

正 12　　〃　　〃　　$= 20 \cdot 3 = 60$

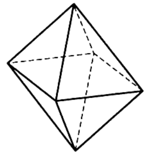
正 20　　〃　　〃　　$= 12 \cdot 5 = 60$



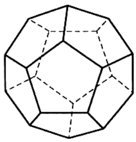
正 4 面体



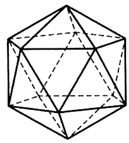
正 6 面体



正 8 面体



正 12 面体



正 20 面体

1.4　正規部分群と剰余群

群 G の元 a, b と部分集合 S に対して，

$$b^a = a^{-1}ba, \qquad S^a = \{a^{-1}xa \mid x \in S\}$$

とおく．

G の部分群 H と G の部分集合 S, T に対して，

$$S^x = T$$

となる H の元 x があるとき，S と T は H で**共役**あるいは H-**共役**であるという．とくに G で共役であるときは，単に共役であるともいう．

群 G の元 a, b の間の関係 $\sim$ を

$a \sim b \Longleftrightarrow a$ と b は**共役** $\Longleftrightarrow \{a\}$ と $\{b\}$ は共役

によって定めると，$\sim$ は G における同値関係となることがやさしく分かる．G の $\sim$ による同値類を G の**共役類**といい，共役類の個数を G の**類数**という．

例 1.4.1

G を集合 Ω 上の置換群とし，Ω の元 α, β に対して $(\alpha)g = \beta$ となる G の元

g があるとする．このとき，固定部分群 G_α と G_β は共役である．

証　明

G_α の任意の元 h に対して，$(\beta)g^{-1}hg=\beta$ となるから，

$$g^{-1}G_\alpha g \subseteqq G_\beta$$

が成り立つ．逆に G_β の任意の元 x に対して，$(\alpha)gxg^{-1}=\alpha$ であるから，$gxg^{-1} \in G_\alpha$ である．よって，$x=g^{-1}(gxg^{-1})g \in g^{-1}G_\alpha g$，それゆえ

$$g^{-1}G_\alpha g \supseteqq G_\beta$$

が成り立つ．したがって，$g^{-1}G_\alpha g=G_\beta$ となり，G_α と G_β は共役である．

集合 Ω 上の置換群 G の元 g が Ω の元 α を元 β に移すとき，すなわち $(\alpha)g=\beta$ であるとき，$\alpha^g=\beta$ と書くことがある．このとき，すべての $h \in G$ に対して

$$(\alpha^h)^{h^{-1}gh}=\beta^h$$

が成り立つ．置換群を扱うときこの記法は便利であり([洋；16] 参照)，写像の合成 $\circ$ を左から行うことが多い1つの理由であろう．

群 G の部分集合 S と部分群 H に対して，

$$N_H(S)=\{g \in H \mid S^g=S\}$$

$$C_H(S)=\{g \in H \mid S \text{ のすべての元 } x \text{ に対して } xg=gx\}$$

とおくと，それらは H の部分群であることがやさしく分かる．$N_H(S)$ を H における S の**正規化群**，$C_H(S)$ を H における S の**中心化群**という．S が1つだけの元からなる集合 $\{a\}$ のとき

$$N_H(\{a\})=C_H(\{a\})$$

となるが，以後これを $C_H(a)$ で表すことにする．

定　理 | 1.4.2

群 G の元 a，部分集合 S，部分群 H に対して次の(1)，(2)が成り立つ．

(1)　S と H-共役な G の部分集合の個数は $|H:N_H(S)|$ である．

(2)　a と H-共役な G の元の個数は $|H:C_H(a)|$ である．

証明

(2)は(1)からいえるので，(1)を示せばよい．

$\{x_1, x_2, \cdots, x_t\}$ を H における $N_H(S)$ の左代表系とすると，

$$H = N_H(S)x_1 + N_H(S)x_2 + \cdots + N_H(S)x_t \qquad (\text{直和})$$

である．$N_H(S)$ の任意の元 g に対して，

$$S^{gx_i} = S^{x_i}$$

が成り立つ．また，$S^{x_i} = S^{x_j}$ であるための必要十分条件は $x_i x_j^{-1} \in N_H(S)$ であるので，$i \neq j$ ならば $S^{x_i} \neq S^{x_j}$ である．したがって，S と H-共役な G の部分集合の個数は t 個である．

群 G の部分群 H が $N_G(H) = G$ をみたすとき，H を G の**正規部分群**といい，$H \trianglelefteq G$ で表す．明らかに1および G は G の正規部分群であり，それらを**自明な正規部分群**という．群 G が自明でない正規部分群をもたないとき，G を**単純群**という．$n \geqq 5$ のとき，交代群 A_n が単純群であることはよく知られている([和；10] 参照)．

群 G において，$C_G(G)$ を G の**中心**といい，$Z(G)$ で表す．明らかに $Z(G)$ は G の正規部分群である．

H が群 G の正規部分群であるとき，G における H の左剰余類全体からなる集合 $H\backslash G$ と右剰余類全体からなる集合 G/H は同じである．そして G/H の任意の元 xH と $yH\,(x, y \in G)$ に対して，

$$(xH)(yH) = x(Hy)H = xyHH = xyH$$

となるので，G/H の元 xyH が一意的に定まる．そして，この演算によって G/H は群となることが分かり，これを G の H による**剰余群**という．なお，群 G/H の単位元は H で，xH の逆元は $x^{-1}H$ である．

例 1.4.3

実数を成分とする n 次正則行列全体は積に関して群であり，これを $GL(n, \boldsymbol{R})$ と書いて，$\boldsymbol{R}$ 上の n 次**一般線形群**という．また，

$$\{A \in GL(n, \boldsymbol{R}) \mid \det A = 1\}$$

は $GL(n, \boldsymbol{R})$ の正規部分群であり，これを $SL(n, \boldsymbol{R})$ と書いて，$\boldsymbol{R}$ 上の n 次**特殊線形群**という．I を n 次単位行列とすると，

$$Z(GL(n, \boldsymbol{R})) = \{aI \mid a \in \boldsymbol{R},\ \ a \neq 0\}$$

$$Z(SL(n, \boldsymbol{R})) = \begin{cases} \{\pm I\} & (n：偶数) \\ \{I\} & (n：奇数) \end{cases}$$

が成り立つ．

証 明

$i \neq j$ に対して，I の (i, j) 成分の 0 を $c \neq 0$ にした行列を $Q_n(i, j\,;\,c)$ とする．$Q_n(i, j\,;\,c)$ は $SL(n, \boldsymbol{R})$ の元なので，$Z(GL(n, \boldsymbol{R}))$ あるいは $Z(SL(n, \boldsymbol{R}))$ の元はそれらと可換でなくてはならない．それを用いることによって，結論が得られる．

例 | 1.4.4

a, b をそれぞれ巡回置換

$$a = (1\ \ 2\ \ 3\ \ 4\ \ 5\ \ 6\ \ 7), \qquad b = (2\ \ 4\ \ 3\ \ 7\ \ 5\ \ 6)$$

とし，$\Omega = \{1, 2, 3, 4, 5, 6, 7\}$ 上の置換群

$$G = \langle a, b \rangle, \qquad N = \langle a \rangle, \qquad H = \langle b \rangle$$

を考える．

$$b^{-1}ab = (1^b, 2^b, 3^b, 4^b, 5^b, 6^b, 7^b) = (1\ \ 4\ \ 7\ \ 3\ \ 6\ \ 2\ \ 5) = a^3$$

$$N \cap H = 1$$

となるので，$N = \langle a \rangle$ は $G = \langle a, b \rangle$ の正規部分群で，G の任意の元は $b^j a^i$ $(0 \leqq i \leqq 6,\ 0 \leqq j \leqq 5)$ という形で一意的に表される．そして，G の N による剰余群は

$$G/N = \{N, bN, b^2N, b^3N, b^4N, b^5N\}$$

となる．

1.5 準同型

群 G_1 から群 G_2 への写像 φ が

$$(xy)\varphi = (x)\varphi\cdot(y)\varphi$$

をすべての $x, y \in G_1$ に対してみたすとき，φ を G_1 から G_2 への**準同型写像**という．G_1 の単位元を 1，G_2 の単位元を e とすると，

$$(1)\varphi\cdot(1)\varphi = (1\cdot 1)\varphi = (1)\varphi$$

より，$(1)\varphi = e$ が成り立つ．そして，任意の $g \in G_1$ に対して

$$(g)\varphi\cdot(g^{-1})\varphi = (1)\varphi = e$$

となるので，$((g)\varphi)^{-1} = (g^{-1})\varphi$ が成り立つ．φ による G_1 の**像** $(G_1)\varphi$ を $\mathrm{Im}\,\varphi$ で表し，e の逆像

$$(e)\varphi^{-1} = \{g \in G_1 \mid (g)\varphi = e\}$$

を $\mathrm{Ker}\,\varphi$ で表し，それを φ の**核**という．$\mathrm{Im}\,\varphi$ は G_2 の部分群で，$\mathrm{Ker}\,\varphi$ は G_1 の部分群であることはやさしく分かる．また，任意の $x \in \mathrm{Ker}\,\varphi$ と任意の $g \in G_1$ に対して，

$$(g^{-1}xg)\varphi = (g^{-1})\varphi(x)\varphi(g)\varphi = ((g)\varphi)^{-1}\cdot e\cdot(g)\varphi = e$$

となるので，$\mathrm{Ker}\,\varphi$ は G_1 の正規部分群である．とくに $\mathrm{Ker}\,\varphi = \{1\}$ ならば，φ は単射である．実際，G_1 の元 x, y に対して，

$$(x)\varphi = (y)\varphi$$

とすると，

$$(x^{-1}y)\varphi = ((x)\varphi)^{-1}(y)\varphi = e$$

から，$x^{-1}y = 1$ すなわち $x = y$ が導かれる．

群 G_1 から群 G_2 への準同型写像 φ が全単射であるとき，φ を G_1 から G_2 の上への**同型写像**という．このとき，G_1 と G_2 は**同型**であるといい，記法として $G_1 \cong G_2$ で表す．

例 | 1.5.1

N が群 G の正規部分群であるとする．このとき，G から剰余群 G/N への写像 φ を，

$$(g)\varphi = gN$$

によって各 $g \in G$ に対して定める．明らかに，φ は G から G/N の上への準同型写像で，$\mathrm{Ker}\,\varphi = N$ である．この φ を G から G/N への**自然な準同型写像**という．

例 | 1.5.2

$\boldsymbol{C}$ の元 1，-1，$\sqrt{-1}$，$-\sqrt{-1}$ からなる集合 G_1 は積に関して群となり，$\{1, 2, 3, 4\}$ 上の置換群 $G_2 = \{1, (1\ \ 2\ \ 3\ \ 4), (1\ \ 3)(2\ \ 4), (1\ \ 4\ \ 3\ \ 2)\}$ と(群として)同型である．

集合 Ω_1 上の置換群 G_1 と集合 Ω_2 上の置換群 G_2 に対して，Ω_1 から Ω_2 への全単射 f と G_1 から G_2 への全単射 φ があって次の条件をみたすとき，G_1 と G_2 は**置換群として同型**であるという：φ は G_1 から G_2 の上への(群としての)同型写像で，Ω_1 の元 α，β と G_1 の元 g に対して，

$$\alpha^g = \beta \Longleftrightarrow ((\alpha)f)^{(g)\varphi} = (\beta)f$$

が成り立つ．

この定義から想像できるだろうが，群としては同型でも置換群としては同型でない2つの置換群はいくらでもある．そして，群としての分類と置換群としての分類は当然異なるものである．

次の2つの定理は基本的に重要である．

定 理 | 1.5.3 ……………… **準同型定理**

φ を群 G_1 から群 G_2 への準同型写像とすると，

$$G_1/\mathrm{Ker}\,\varphi \cong \mathrm{Im}\,\varphi$$

が成り立つ．

証 明

G_1 の任意の元 g と $\mathrm{Ker}\,\varphi$ の任意の元 x に対して，

$$(gx)\varphi = (g)\varphi(x)\varphi = (g)\varphi \in \mathrm{Im}\,\varphi$$

となるので，$G_1/\mathrm{Ker}\,\varphi$ の各元 $g\,\mathrm{Ker}\,\varphi$ を $(g)\varphi$ に対応させる $G_1/\mathrm{Ker}\,\varphi$ から

$\mathrm{Im}\,\varphi$ の上への写像 $\overline{\varphi}$ が定義できる.

任意の $a\,\mathrm{Ker}\,\varphi$, $b\,\mathrm{Ker}\,\varphi \in G/\mathrm{Ker}\,\varphi$ に対して,

$$((a\,\mathrm{Ker}\,\varphi)(b\,\mathrm{Ker}\,\varphi))\overline{\varphi} = (ab\,\mathrm{Ker}\,\varphi)\overline{\varphi} = (ab)\varphi = (a)\varphi(b)\varphi$$

となるので, $\overline{\varphi}$ は準同型写像である. また,

$$\mathrm{Ker}\,\overline{\varphi} = \{x\,\mathrm{Ker}\,\varphi \mid (x)\varphi \text{ は } G_2 \text{ の単位元}\} = \{\ker\varphi\}$$

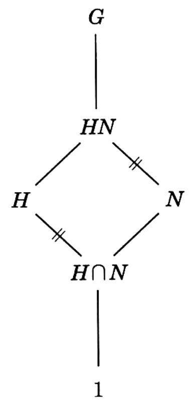
となるので, $\overline{\varphi}$ は単射である. したがって, $\overline{\varphi}$ は $G_1/\mathrm{Ker}\,\varphi$ から $\mathrm{Im}\,\varphi$ の上への同型写像である.

定 理 | 1.5.4 ……………………………………………… **同型定理**

N を群 G の正規部分群, H を G の部分群とするとき, HN は G の部分群で, $H\cap N$ は H の正規部分群である. そして,

$$HN/N \cong H/H\cap N$$

が成り立つ(下図参照).



証 明 ………………………………………………

$$(HN)(HN) = (HH)(NN) = HN$$

となるので, HN は演算に関して閉じている. また, 明らかに $1\in HN$ が成り立ち, HNの任意の元 $hx\,(h\in H,\ x\in N)$ に対して,

$$(hx)^{-1} = x^{-1}h^{-1} \in Nh^{-1} = h^{-1}N$$

となる. よって, HN は G の部分群である. 一方, $H\cap N$ が H の正規部分群

であることはやさしく分かる．

次に，φ を G から G/N への自然な準同型写像とすると，φ の定義域を H に制限した φ_H は H から HN/N の上への準同型写像となる．ここで，$\mathrm{Ker}\,\varphi_H = H \cap N$ となるので，定理 1.5.3 を用いて

$$HN/N \cong H/H \cap N$$

を得る．

例 1.5.5

例 1.4.3 で定めた $GL(n, \boldsymbol{R})$ に対し，その各元 A を行列式 $\det A$ に対応させる写像 φ は，$GL(n, \boldsymbol{R})$ から $\boldsymbol{R}^* = \boldsymbol{R} - \{0\}$ の上への準同型写像である(例 1.2.1(ウ)参照)．そして，

$$\mathrm{Ker}\,\varphi = \{A \in GL(n, \boldsymbol{R}) \mid \det A = 1\}$$

となるので，

$$GL(n, \boldsymbol{R})/SL(n, \boldsymbol{R}) \cong \boldsymbol{R}^*$$

を得る．

例 1.5.6

$\{1, 2, 3, 4\}$ 上の対称群を G とし，置換群 N, H を

$$N = \{1,\ (1\ \ 2)(3\ \ 4),\ (1\ \ 3)(2\ \ 4),\ (1\ \ 4)(2\ \ 3)\}$$

$$H = G_4 \quad (G \text{ における 4 の固定部分群})$$

$$= \{1,\ (1\ \ 2),\ (1\ \ 3),\ (2\ \ 3),\ (1\ \ 2\ \ 3),\ (1\ \ 3\ \ 2)\}$$

によって定める．N は G の正規部分群で，$H \cap N = 1$ なので，

$$HN/N \cong H/H \cap N \cong H$$

を得る．したがって，

$$|G| \geqq |HN| = |H| \cdot |N| = 6 \times 4 = |G|$$

となるので，$G = HN$ そして $G/N \cong H$ が成り立つ．

群 G から G の上への同型写像を G の**自己同型写像**という．G の自己同型写像全体からなる集合を $\mathrm{Aut}(G)$ と書くと，$\mathrm{Aut}(G)$ は写像の合成に関して群

となり，これを G の**自己同型群**という．いま，a を G の任意に固定した元とする．このとき，G の各元 x に対して，x を $x^a = a^{-1}xa$ に対応させる写像 σ_a を定めると，σ_a は G の自己同型写像となる．一般に σ_a を a による G の**内部自己同型写像**というが，それら全体からなる集合

$$\mathrm{Inn}(G) = \{\sigma_a \mid a \in G\}$$

は明らかに $\mathrm{Aut}(G)$ の部分群である．さらに，$\mathrm{Inn}(G)$ の任意の元 σ_a と $\mathrm{Aut}(G)$ の任意の元 τ に対して，

$$\tau^{-1}\sigma_a\tau = \sigma_{(a)\tau} \in \mathrm{Inn}(G)$$

となることがやさしく分かる．よって，$\mathrm{Inn}(G)$ は $\mathrm{Aut}(G)$ の正規部分群である．剰余群 $\mathrm{Aut}(G)/\mathrm{Inn}(G)$ を G **外部自己同型群**のといい，それを $\mathrm{Out}(G)$ で表す．

K を群 G の部分群とするとき，K が G の正規部分群であるための必要十分条件は，すべての $\sigma \in \mathrm{Inn}(G)$ に対して $(K)\sigma = K$ が成り立つことである．そして，すべての $\tau \in \mathrm{Aut}(G)$ に対して $(K)\tau = K$ が成り立つとき，K を G の**特性部分群**という．

定　理 | 1.5.7

N が群 G の正規部分群で，K が N の特性部分群ならば，K は G の正規部分群である．

証　明

G の任意の元 g に対して，g による G の内部自己同型写像 σ_g によって N は集合として固定される．すなわち，

$$(N)\sigma_g = N$$

となるが，σ_g を N に制限した写像は明らかに N の自己同型写像である．よって仮定により，

$$(K)\sigma_g = K$$

を得る．したがって，K は G の正規部分群である．

例 1.5.8

G を a で生成された位数 n の巡回群とすると，$\mathrm{Aut}(G)$ は位数 $\varphi(n)$ の可換群となる．ここで，φ は**オイラー関数**である．すなわち，

$$\varphi(n)=\begin{cases}1 & (n=1\text{ のとき})\\ |\{m\in \boldsymbol{N} \mid 1\leqq m<n,\ (m,n)=1\}| & (n>1\text{ のとき})\end{cases}$$

である．

証明

最初に，$n=1$ の場合は明らかなので，$n>1$ を仮定する．

$\mathrm{Aut}(G)$ の任意の元 σ をとると，明らかに $G=\langle(a)\sigma\rangle$ である．いま，

$$(a)\sigma=a^t \qquad (1\leqq t\leqq n-1)$$

とおくと，もし $(t,n)\neq 1$ ならば $(a)\sigma$ は G を生成しない．よって，$(t,n)=1$ でなければならない．一方，$(t,n)=1$ となる $t\ (1\leqq t\leqq n-1)$ に対して，

$$(a^i)\tau=a^{it} \qquad (i=0,1,\cdots,n-1)$$

とおくと，$\tau\in\mathrm{Aut}(G)$ である．したがって，$|\mathrm{Aut}(G)|=\varphi(n)$ を得る．

次に，$\mathrm{Aut}(G)$ の任意の元 σ，τ に対して，

$$(a)\sigma=a^s, \qquad (a)\tau=a^t \qquad (1\leqq s,\ t\leqq n-1)$$

とおくと，

$$(a)\sigma\tau=(a^s)\tau=(a^t)^s=(a^s)^t=(a^t)\sigma=(a)\tau\sigma$$

となる．したがって，

$$\sigma\tau=\tau\sigma$$

であり，$\mathrm{Aut}(G)$ は可換群となる．

1.6 直積と半直積

n 個の群 $G_1, G_2, \cdots, G_n$ の直積集合

$$G=G_1\times G_2\times\cdots\times G_n=\{(x_1,x_2,\cdots,x_n)\mid x_i\in G_i\}$$

を考える．G の任意の元 $a=(a_1,a_2,\cdots,a_n)$，$b=(b_1,b_2,\cdots,b_n)$ に対する演算を

$$ab = (a_1b_1, a_2b_2, \cdots, a_nb_n)$$

によって定義すると G は群となり，それを群 $G_1, G_2, \cdots, G_n$ の**直積**という．G の単位元は $(e_1, e_2, \cdots, e_n)$ で (e_i は G_i の単位元)，$(x_1, x_2, \cdots, x_n)$ の逆元は $(x_1^{-1}, x_2^{-1}, \cdots, x_n^{-1})$ である．いま，各 i ($1 \leqq i \leqq n$) に対して

$$H_i = \{(e_1, \cdots, e_{i-1}, h, e_{i+1}, \cdots, e_n) \mid h \in G_i\}$$

と定めると，各 H_i は G の正規部分群で，

$$H_i \cong G_i$$

$$G = H_1H_2\cdots H_n$$

$$(H_1H_2\cdots H_{i-1}) \cap H_i = 1 \qquad (i = 1, 2, \cdots, n)$$

をみたす．

逆に $H_1, H_2, \cdots, H_n$ が群 G の正規部分群で(上記の $H_1, H_2, \cdots, H_n$ や G とは無関係)，

$$G = H_1H_2\cdots H_n$$

$$(H_1H_2\cdots H_{i-1}) \cap H_i = 1 \qquad (i = 2, \cdots, n)$$

をみたすならば，

$$G \cong H_1 \times H_2 \times \cdots \times H_n$$

が成り立つ．実際，群 $H_1 \times H_2 \times \cdots \times H_n$ の各元 $(x_1, x_2, \cdots, x_n)$ を G の元 $x_1x_2\cdots x_n$ に対応させる写像を φ とすると，$H_1 \times H_2 \times \cdots \times H_n$ の任意の元 $a = (a_1, a_2, \cdots, a_n)$，$b = (b_1, b_2, \cdots, b_n)$ に対して，

$$(ab)\varphi = (a)\varphi(b)\varphi$$

は次のようにして示せる．

$$b_1^{-1}a_2^{-1}b_1a_2 = (b_1^{-1}a_2^{-1}b_1)a_2 = b_1^{-1}(a_2^{-1}b_1a_2)$$

は H_2 かつ H_1 の元なので，それは1に等しい．よって，

$$b_1a_2 = a_2b_1$$

となる．以下同様に $i = 3, 4, \cdots, n$ に対して，

$$(b_1b_2\cdots b_{i-1})^{-1}a_i^{-1}(b_1b_i\cdots b_{i-1})a_i \in H_1H_2\cdots H_{i-1} \cap H_i = 1$$

なので，

$$b_1b_2\cdots b_{i-1}a_i = a_ib_1b_2\cdots b_{i-1}$$

となる．したがって，

$$\begin{aligned}(ab)\varphi &= ((a_1, a_2, \cdots, a_n)(b_1, b_2, \cdots, b_n))\varphi \\ &= (a_1b_1, a_2b_2, \cdots, a_nb_n)\varphi \\ &= a_1b_1a_2b_2a_3b_3\cdots a_nb_n \\ &= a_1a_2b_1b_2a_3b_3\cdots a_nb_n \\ &\qquad \vdots \\ &= a_1a_2\cdots a_nb_1b_2\cdots b_n \\ &= (a)\varphi(b)\varphi\end{aligned}$$

が成り立つ．また，

$$(x_1, x_2, \cdots, x_n)\varphi = 1$$

とすると，

$$x_1x_2\cdots x_{n-1} = x_n^{-1} \in H_1H_2\cdots H_{n-1} \cap H_n$$

であるから $x_n = 1$ を得る．同様にして，$x_{n-1} = 1$，$x_{n-2} = 1$，…，$x_1 = 1$ を得る．そこで準同型定理を用いて，

$$G = H_1H_2\cdots H_n \cong H_1 \times H_2 \times \cdots \times H_n$$

が成り立つ．

一般に上式の関係が成り立つとき，G と $H_1 \times H_2 \times \cdots \times H_n$ を同一視して

$$G = H_1 \times H_2 \times \cdots \times H_n$$

と書き，G は $H_1, H_2, \cdots, H_n$ の**直積**であるという．

例 | 1.6.1

巡回置換 $(1\ \ 2\ \ 3\ \ 4\ \ 5\ \ 6)$ で生成される巡回群 G は，次のように2つの部分群の直積として表せる．

$$G = \langle(1\ \ 4)(2\ \ 5)(3\ \ 6)\rangle \times \langle(1\ \ 3\ \ 5)(2\ \ 4\ \ 6)\rangle$$

群 G の正規部分群 N と部分群 H があって，

$$G = HN, \qquad H \cap N = 1$$

をみたしているとき，G は正規部分群 N と部分群 H の**半直積**であるという．そして H の任意の元 h に対して，h による G の内部自己同型写像 σ_h を N に

制限したものは N の自己同型写像を引き起こしている．

逆に K, N を群とし，K の各元が N の自己同型写像を引き起こしているとする．厳密に述べると，K から $\mathrm{Aut}(N)$ への準同型写像 φ があって，φ を通して K の各元の N 上の作用を考える(以下 φ は省略)．このとき，K と N の直積集合

$$G = K \times N$$

に次のように演算を定めると，G は群になる：G の任意の元 $g_1 = (k_1, n_1)$，$g_2 = (k_2, n_2)\,(k_i \in K,\ n_i \in N)$ に対して，

$$g_1 g_2 = (k_1 k_2, n_1^{k_2} n_2),$$

ただし $n_1^{k_2}$ は k_2 による n_1 の像である．実際，G の元 $g_i = (k_i, n_i)\,(i = 1, 2, 3)$ に対して，

$$\begin{aligned}(g_1 g_2)\, g_3 &= (k_1 k_2, n_1^{k_2} n_2)\,(k_3, n_3)\\ &= (k_1 k_2 k_3, (n_1^{k_2} n_2)^{k_3} n_3)\\ &= (k_1 k_2 k_3, n_1^{k_2 k_3} n_2^{k_3} n_3)\\ &= (k_1, n_1)\,(k_2 k_3,\ n_2^{k_3} n_3)\\ &= g_1 (g_2 g_3)\end{aligned}$$

が成り立つ．また，G の単位元は $(1, 1)$ で，$g = (k, n)$ の逆元は $(k^{-1}, (n^{-1})^{k^{-1}})$ である．

ここで G の部分群

$$\tilde{N} = \{(1, n) \mid n \in N\}, \qquad \tilde{K} = \{(k, 1) \mid k \in K\}$$

を考えると，$\tilde{N}$ と N は同型で，$\tilde{K}$ と K は同型である．さらに

$$G = \tilde{K}\tilde{N}, \qquad \tilde{K} \cap \tilde{N} = 1, \qquad \tilde{N} \trianglelefteq G$$

が成り立つので，G は正規部分群 $\tilde{N}$ と部分群 $\tilde{K}$ の半直積である．この関係によって，G は正規部分群 N と部分群 K の半直積であると見なせる．

例 1.6.2

例 1.4.4 における群 $G = \langle a, b \rangle$ は，正規部分群 $N = \langle a \rangle$ と部分群 $H = \langle b \rangle$ の半直積である．ただし，

$$a = (1\ \ 2\ \ 3\ \ 4\ \ 5\ \ 6\ \ 7), \qquad b = (2\ \ 4\ \ 3\ \ 7\ \ 5\ \ 6).$$

なお，群 G が部分群 H_1 と H_2 の直積であるとき，G は明らかにそれらの半直積である．

1.7 p-群

定理 1.3.1 より，任意の有限群 G に対して，その部分群の位数は $|G|$ の約数である．反対に $|G|$ の約数に対しては，それを位数とする部分群は必ずしも存在するものではない．本節で扱う p-群は有限群に関して必ず存在するもので (定理 1.7.2 参照)，有限群の学習にとって大切な基礎である．

位数が素数 p の累乗(巾(べき))である有限群を **p-群**という．明らかに，単位群は位数が p^0 の p-群である．有限群 G の位数 $|G|$ が，

$$|G| = p^s m, \qquad (p, m) = 1$$

と表されるとき，位数 p^s の G の p-部分群をとくに G の**シロー p-部分群**という．最初に次の定理 1.7.1 を述べるが，定理 1.7.2 の後に読まれてもよい．

定理 | 1.7.1

P を 1 と異なる p-群とすると，中心 $Z(P)$ は 1 と異なる．また，Q を P の真部分群とすると，

$$Q < N_P(Q) \qquad (P \text{ における } Q \text{ の正規化群})$$

が成り立つ．

証明

P の任意の元 a に対して，定理 1.4.2 より a を含む共役類の元の個数は $|P : C_P(a)|$ であり，これは p の巾である．いま P の類数を m とし，すべての共役類を $C_1=\{1\}, C_2, \cdots, C_m$ とすると，

$$P = C_1 + C_2 + \cdots + C_m \qquad (\text{直和})$$

と表せる．したがって，

$$|P| = 1 + |C_2| + \cdots + |C_m| \equiv 0 \pmod p$$

となるが，各 $|C_i|$ は p の巾である．もしすべての $i\ (\geqq 2)$ について $|C_i| \geqq p$ とすると，$|P| \equiv 1 \pmod p$ となり矛盾である．よって，ある $i\ (\geqq 2)$ について

$|C_i|=1$ でなければならない．それゆえ $|Z(P)|>1$ である．

次に後半を示すが，$1<Q$ としてよい．P の任意の元 a に対して集合 QaQ を考えると，

$$|Q| \leqq |QaQ| = |a^{-1}QaQ| = |Q^aQ|$$

が成り立つ．$K = Q^a \cap Q$ とおくと K は P の部分群である．ここで Q^a における K の右代表系を $\{a_1, a_2, \cdots, a_s\}$ とすると，$s = |Q^a : K|$ は p の巾で，

$$Q^a = a_1K + a_2K + \cdots + a_sK \qquad (\text{直和})$$

と表せる．そして，

$$Q^aQ = \bigcup_{i=1}^{s} a_iQ$$

となるが，上式右辺は直和である．実際，

$$a_iy = a_jy' \qquad (y, y' \in Q)$$

とすると，

$$a_i^{-1}a_j \in Q^a \cap Q = K$$

となるので，$i=j$ でなければならない．したがって，$|QaQ|$ は $|Q|$ の倍数かつ p の巾である．

一方，P の元 x, x' に対して，$QxQ \cap Qx'Q \neq \emptyset$ ならば，$QxQ = Qx'Q$ となることが容易に分かる．よって，P のある元 $x_1, x_2, \cdots, x_t$ に対し，

$$P = Qx_1Q + Qx_2Q + \cdots + Qx_tQ \qquad (\text{直和})$$

と表されることになる．ここで，$x_1 = 1$ としてよいので，

$$|P| = |Q| + |Qx_2Q| + \cdots + |Qx_tQ|$$
$$|P|/|Q| = 1 + |Qx_2Q|/|Q| + \cdots + |Qx_tQ|/|Q|$$

を得る．もしすべての $i\ (\geqq 2)$ について $|Qx_iQ|/|Q| \geqq p$ とすると，上式右辺 $\equiv 1 \pmod p$ となり矛盾である．したがって，ある $i\ (\geqq 2)$ について

$$|Q^{x_i}Q| = |Qx_iQ| = |Q|$$

でなければならない．これは上の議論で $s=1$ の場合になるので，$x_i \in N_P(Q)$ である．よって，$Q < N_P(Q)$ が成り立つ．

定理 1.7.2 の前に置換群に関する簡単な言葉を約束する．集合 Ω 上の置換

群 G に関して，Ω 上に次のような関係 $\sim$ を定める：Ω の元 α, β に対して，

$$\alpha \sim \beta \Longleftrightarrow (\alpha)g = \beta \text{ となる } G \text{ の元 } g \text{ が存在.}$$

明らかに $\sim$ は Ω 上の同値関係で，各同値類を G の(Ω における)**軌道**，または G-**軌道**という．Δ を G-軌道とするとき，$|\Delta|$ を Δ の**長さ**という．明らかに，Ω の元 α を含む G の軌道は $(\alpha)G$ である．

定　理｜1.7.2 ……………………………… **シローの定理**

G を位数が $p^s m$ の有限群とすると，G において次の(1)，(2)が成り立つ．ただし，p は素数で $(p, m) = 1$ とする．

（1）　任意の整数 t $(0 \leqq t \leqq s)$ に対して，位数が p^t の p-部分群の個数を $n(t)$ とすると，$n(t) \equiv 1 \pmod p$ である．とくに，$n(t) \geqq 1$ である．

（2）　P を任意のシロー p-部分群とし，Q を位数が $p^t (0 \leqq t \leqq s)$ の任意の p-部分群とすると，Q は P と共役なあるシロー p-部分群に含まれる．とくに，すべてのシロー p-部分群は互いに共役である．

証　明 ………………………………

（1）　$|G| = p^t q$，$\Omega = \{X \mid X \subseteqq G,\ |X| = p^t\}$ とおく．$q = 1$ のときは $n(t) = 1$ なので，以下 $q > 1$ とする．Ω は p^t 個の元からなる部分集合全体の集合なので，

$$|\Omega| = \binom{p^t q}{p^t}$$

である．G の任意の元 g に対して，Ω の各元 X を $(X)g$ に対応させる Ω 上の置換 $\bar{g}$ が定まる．この対応によって G から S^{Ω} への写像 φ が定まるが，φ は単射である．実際，G の異なる任意の 2 元 g, h に対して，

$$G \supsetneqq X, \quad |X| = p^t, \quad X \ni g^{-1}, \quad X \not\ni h^{-1}$$

をみたす X があるので，$\bar{g} \neq \bar{h}$ となる．さらに φ は準同型写像なので，G と $\mathrm{Im}\,\varphi$ は群として同型である．そこで，以下 G と Ω 上の置換群 $\mathrm{Im}\,\varphi$ を同一視して考えることにする．

G の Ω における軌道全体を Ω_1, Ω_2, …, Ω_r とし，X_i を Ω_i の元とすると (1

$\leqq i \leqq r$)，定理 1.3.2 より

$$|\Omega_i| = |G : G_{X_i}|$$

$$|\Omega_1| + |\Omega_2| + \cdots + |\Omega_r| = \binom{p^t q}{p^t}$$

である．いま $(X_i)G_{X_i} = X_i$ であるので，各 i に対して

$$X_i = x_{i1}G_{X_i} + x_{i2}G_{X_i} + \cdots + x_{ij_i}G_{X_i} \qquad (\text{直和})$$

をみたす $x_{i1}, x_{i2}, \cdots, x_{ij_i} \in X_i$ が存在する．よって，

$$|G_{X_i}| \cdot j_i = |X_i| = p^t$$

となることから，

$$|G_{X_i}| = p^{e_i} \qquad (0 \leqq e_i \leqq t)$$

を得る．そこで，もし $e_i < t$ ならば

$$|\Omega_i| = |G : G_{X_i}| \equiv 0 \pmod{pq}$$

であり，もし $e_i = t$ ならば

$$|\Omega_i| = |G : G_{X_i}| = q$$

となる．したがって，

$$|\Omega| = \binom{p^t q}{p^t} \equiv q \, |\{i \mid |\Omega_i| = q\}| \pmod{pq}$$

が成り立つ．

次に，G の位数 p^t の任意の部分群 H は必ず $|\Omega_i| = q$ となるある Ω_i に含まれ，そして $|\Omega_j| = q$ をみたす Ω_j は G の唯一の位数 p^t の部分群 K を元としてもつ．実際，

$$|\{Hg \mid g \in G\}| = q, \qquad H \in \{Hg \mid g \in G\}$$

である．一方，$X_j \in \Omega_j$ の元 x_j に対して $X_j = x_j G_{X_j}$ となるので，G_{X_j} と共役な群 $K = x_j G_{X_j} x_j^{-1}$ は

$$K = X_j x_j^{-1} \in \Omega_j$$

をみたす．また，もし位数 p^t の部分群 L も Ω_j の元ならば，

$$Kx = L$$

となる G の元 x が存在し，$K \ni 1$ より $L \ni x$ である．よって，

$$K = Lx^{-1} = L$$

を得る．

以上から，位数 p^t の部分群の個数と $|\Omega_i| = q$ となる軌道の個数は等しくなるので，

$$|\Omega| = \binom{p^t q}{p^t} \equiv q \cdot n(t) \pmod{pq}$$

が成り立つ．ここで，とくに G が位数 $p^t q$ の巡回群としても上式は成り立つので，定理 1.2.6 よりその場合は $n(t) = 1$ である．すなわち

$$\binom{p^t q}{p^t} \equiv q \pmod{pq}$$

である．したがって，位数が $p^t q$ の一般の群 G に対して，

$$\binom{p^t q}{p^t} \equiv q \cdot n(t) \equiv q \pmod{pq}$$

となるので，

$$n(t) \equiv 1 \pmod{p}$$

を得る．

（2）　$G = P$ のときは明らかに成り立つので，以下 $G > P$ とする．G における P の左剰余類全体からなる集合 $P\backslash G$ を Ω とし，G の任意の元 g に対して，Ω の各元 Px を Pxg に対応させる Ω 上の置換 $\bar{g}$ が定まる．この対応によって G から S^{Ω} への写像 φ が定まり，φ は準同型写像である．Ω 上の置換群 $(Q)\varphi$ を $\bar{Q}$ とすると，

$$|\bar{Q}| = |Q|/|\mathrm{Ker}\,\varphi \cap Q|$$

となるから $\bar{Q}$ は p-群である．また，

$$|\Omega| = p^s m / p^s = m$$

であるから，$|\Omega|$ は p と互いに素である．$\bar{Q}$ の Ω における軌道全体を $\Omega_1, \Omega_2, \cdots, \Omega_r$ とすると，定理 1.3.2 より各 $|\Omega_i|$ は $|\bar{Q}|$ の約数となる．ここで，

$$|\Omega_1| + |\Omega_2| + \cdots + |\Omega_r| = |\Omega| \not\equiv 0 \pmod{p}$$

なので，ある j に対して $|\Omega_j| = 1$ である．いま $\Omega_j = Px$ とおくと，

$$PxQ = Px$$

$$(x^{-1}Px)Q = x^{-1}Px$$

となるので，Q は P と共役な群 $x^{-1}Px$ に含まれることになる．

例 | 1.7.3

単位元以外の位数がすべて素数 p となる可換 p-群を**基本可換群**という．

P を位数が p^n $(n \geqq 1)$ の基本可換群とするとき，x_1 を $P-\{1\}$ の元とすれば，$\langle x_1 \rangle$ は P の正規部分群である．次に x_2 を $P-\langle x_1 \rangle$ の元とすれば，$\langle x_2 \rangle$ も P の正規部分群で，

$$\langle x_1, x_2 \rangle = \langle x_1 \rangle \times \langle x_2 \rangle$$

となり，これも P の正規部分群である．次に x_3 を $P-\langle x_1, x_2 \rangle$ の元とすれば，$\langle x_3 \rangle$ も P の正規部分群で，

$$\langle x_1, x_2, x_3 \rangle = \langle x_1 \rangle \times \langle x_2 \rangle \times \langle x_3 \rangle$$

となり，これも P の正規部分群である．上の議論をくり返すことにより，

$$P = \langle x_1 \rangle \times \langle x_2 \rangle \times \cdots \times \langle x_n \rangle$$

となる $x_1, x_2, \cdots, x_n$ の存在が分かる．

したがって，位数 p^n $(n \geqq 1)$ の基本可換群は，n 個の位数 p の巡回群の直積として表せる．

1.8 有限体

具体的な例を構成するとき，その土台となるものは当然実在するものである．組合せ構造における重要な例は，有限体を土台として構成されるものが多い．詳しい証明は代数学の専門書等に譲ることにして([和；10] 参照)，本節では環，体の定義から始まって有限体の重要な性質を紹介する．さて，群は集合にいくつかの条件をみたす 1 つの演算が定められているものであった．環そして体は，定められている演算の個数は 2 つである．

加法 $+$ と乗法・の 2 つの演算が定義された集合 R が**環**であるとは，次の条件(1)，(2)，(3)，(4)をみたすことである．

(1) R は加法 $+$ に関して加法群である．

(2) R は乗法・に関して結合法則が成り立つ．

(3) R は**分配法則**をみたす．すなわち，R の任意の元 a, b, c に対して

$$a(b+c) = ab+ac, \qquad (a+b)c = ac+bc$$

が成り立つ．

（４） R には零元 0 とは異なる元 1 があって，R の任意の元 x に対して

$$1x = x1 = x$$

をみたす．1 を R の**単位元**といい，それは唯一であることが分かる．

なお本書とは異なって，環の公理から(4)を外す場合もあることを注意しよう．また，環 R が次の(5)をみたすとき，R を**可換環**という．

（５） R は乗法・に関して交換法則が成り立つ．

環 R に対して，$R^* = R-\{0\}$ が乗法・に関して群になるとき R を**斜体**といい，R^* が乗法・に関して可換群になるとき R を**体**あるいは**可換体**という．

例 1.8.1

（ア） $\boldsymbol{Z}$ は体ではないが，可換環であり，それを**有理整数環**という．$\boldsymbol{Q}, \boldsymbol{R}, \boldsymbol{C}$ は体であり，それぞれ**有理数体**，**実数体**，**複素数体**という．また，$\boldsymbol{Z}, \boldsymbol{Q}, \boldsymbol{R}, \boldsymbol{C}$ の元をそれぞれ係数とする１変数 x の多項式全体からなる集合 $\boldsymbol{Z}[x]$, $\boldsymbol{Q}[x]$, $\boldsymbol{R}[x]$, $\boldsymbol{C}[x]$ は可換環である．

（イ） 実数を係数とする n 次正方行列全体の集合を $M(n, \boldsymbol{R})$ とすると $(n \geqq 2)$，$M(n, \boldsymbol{R})$ は環であるが可換環ではない．$M(n, \boldsymbol{R})$ の零元，単位元はそれぞれ n 次零行列 O_n，n 次単位行列 I_n である．

環 R において，零元 0 と任意の元 x に対して，

$$0x = (0+0)x = 0x+0x$$

であるから，$0x = 0$ が成り立つ．また同様にして，$x0 = 0$ も成り立つ．

一方，$M(2, \boldsymbol{R})$ において

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

が成り立つように，一般の環においては零元でない元 a, b に対して，$ab = 0$ となることがある．

可換環 R が**整域**であるとは，零元でない R の元 a, b に対して必ず $ab \neq 0$ が成り立つことである．例 1.8.1 (ア) で述べた例はすべて整域である．とくに，

R が体ならば R は整域である．実際，a, b を 0 でない R の元とし，$ab=0$ とすると，

$$b = 1b = (a^{-1}a)b = a^{-1}(ab) = a^{-1}0 = 0$$

となるので矛盾である．なお，定理 1.8.2 で例示するように，可換環は必ずしも整域ではない．

さて環に関しても，1.5 節で群に関して学んだ準同型定理と同様な定理が成り立つ．次に，それについて学ぶことにする．

環 R の部分集合 I が次の(1)，(2)をみたすとき，I を R の**左イデアル**という．

（1） I は R の加法 $+$ に関して加法群である．

（2） R の任意の元 r と I の任意の元 a に対して，$ra \in I$ である．

また，I が(1)と次の(3)をみたすとき，I を R の**右イデアル**という．

（3） R の任意の元 r と I の任意の元 a に対して，$ar \in I$ である．

さらに，I が(1)，(2)，(3)をみたすとき，I を R の**両側イデアル**，あるいは単に**イデアル**という．

環 R の真部分集合 I が両側イデアルとするとき，演算 $+$ に関する剰余群 R/I を考えよう．R/I の任意の元 $a+I$，$b+I$ に対して，

$$(a+I)+(b+I) = a+b+I$$

である．さらに，I が両側イデアルなので

$$(a+I)(b+I) \subseteqq ab+I$$

が成り立つことも分かる．なお，上式では必ずしも等号が成立しないことに注意したい．しかしながら上式によって，R/I に乗法も定義できることになる．そして R/I の任意の元 $a+I$ を $\bar{a}$ で表すことにすれば，R/I の任意の元 $\bar{a}$，$\bar{b}$，$\bar{c}$ に対して，

$$(\bar{a}\,\bar{b})\,\bar{c} = \bar{a}(\bar{b}\,\bar{c})$$

$$\bar{a}(\bar{b}+\bar{c}) = \bar{a}\,\bar{b}+\bar{a}\,\bar{c}, \qquad (\bar{a}+\bar{b})\,\bar{c} = \bar{a}\,\bar{c}+\bar{b}\,\bar{c}$$

が成り立ち，I は単位元となる．したがって R/I は環となり，それを R の I による**剰余環**という．

n を 2 以上の整数とするとき，$n\boldsymbol{Z} = \{n \text{ の倍数全体}\}$ は有理整数環 $\boldsymbol{Z}$ のイ

デアルで，$\boldsymbol{Z}/n\boldsymbol{Z}$ は n 個の元 $\overline{0}, \overline{1}, \cdots, \overline{n-1}$ からなる可換環である．この環を $\boldsymbol{Z}_n$ で表すと，次の定理を得る．

定理 1.8.2

n を 2 以上の整数とするとき，次の(1)，(2)が成り立つ．

（1） n が素数でないとき，$\boldsymbol{Z}_n$ は可換環であるが整域ではない．

（2） n が素数のとき，$\boldsymbol{Z}_n$ は体となる．

証明

（1） $n = ab$ $(1 < a,\ 1 < b)$ と表されると，$\overline{a}\ \overline{b} = \overline{0}$ となるので，$\boldsymbol{Z}_n$ は整域ではない．

（2） $\boldsymbol{Z}_n$ の $\overline{0}$ とは異なる任意の元 $\overline{i}$ に対して，

$$\overline{i}\{\overline{0}, \overline{1}, \cdots, \overline{n-1}\} = \{\overline{0}, \overline{1}, \cdots, \overline{n-1}\}$$

である．実際，$\overline{i}\ \overline{j} = \overline{i}\ \overline{k}$ とすると，

$$\overline{i}\ \overline{j} - \overline{i}\ \overline{k} = \overline{i}\,(\overline{j} - \overline{k}) = \overline{i}\,(\overline{j-k}) = \overline{i\,(j-k)} = \overline{0}$$

となるので，$i(j-k)$ は n の倍数となり，よって $j-k$ が n の倍数になる．すなわち，$\overline{i}\ \overline{j} = \overline{i}\ \overline{k}$ ならば $\overline{j} = \overline{k}$ である．したがって，乗法に関する $\overline{i}$ の逆元は必ず存在する．それゆえ $\boldsymbol{Z}_n$ は体となる．

環 R_1 から環 R_2 への写像 φ が，

$$(x+y)\varphi = (x)\varphi + (y)\varphi, \qquad (xy)\varphi = (x)\varphi\,(y)\varphi$$

をすべての $x, y \in R_1$ に対してみたし，

$$(1)\varphi = 1' \qquad (1, 1' \text{ はそれぞれ } R_1, R_2 \text{ の単位元})$$

をみたすとき，φ を R_1 から R_2 への(環としての)**準同型写像**という．さらに φ が全単射であるとき，φ を R_1 から R_2 の上への**同型写像**であるという．このとき，R_1 と R_2 は(環として)**同型**であるといい，記法として $R_1 \cong R_2$ で表す．

環 R_1 から環 R_2 への準同型写像 φ に対して，φ による R_1 の**像** $(R_1)\varphi$ を $\mathrm{Im}\,\varphi$ で表し，R_2 の零元 0 の逆像を $\mathrm{Ker}\,\varphi$ で表し，それを φ の**核**という．

環 R の部分集合 S が次の条件(1)，(2)，(3)をみたすとき，S を R の**部分環**

という．

（1） S は R の部分加法群．

（2） S の任意の元 x, y に対し $xy \in S$ である．

（3） S は R の単位元 1 を含む．

もし環 R の部分環 S が体になるとき，S を R の**部分体**という．

以上の準備のもとで，次の 2 つの定理が成り立つ．

定 理 | 1.8.3

φ を環 R_1 から環 R_2 への準同型写像とすると，$\mathrm{Ker}\,\varphi$ は R_1 の両側イデアルで，$\mathrm{Im}\,\varphi$ は R_2 の部分環である．

証 明

$\mathrm{Ker}\,\varphi$ が R_1 の部分加法群であることは明らか．R_1 の任意の元 r と $\mathrm{Ker}\,\varphi$ の任意の元 a に対して，

$$(ra)\varphi = (r)\varphi\,(a)\varphi = (r)\varphi\cdot 0 = 0.$$

同様にして $(ar)\varphi = 0$ も分かるので，$\mathrm{Ker}\,\varphi$ は R_1 の両側イデアルである．次に $\mathrm{Im}\,\varphi$ は R_2 の部分加法群である．また，R_1 の任意の元 x, y と R_1 の単位元 1 に対して，

$$(x)\varphi\,(y)\varphi = (xy)\varphi \in \mathrm{Im}\,\varphi, \qquad (1)\varphi \in \mathrm{Im}\,\varphi$$

であるので，$\mathrm{Im}\,\varphi$ は R_2 の部分環である．

定 理 | 1.8.4 ……準同型定理

φ を環 R_1 から環 R_2 への準同型写像とすると，

$$R_1/\mathrm{Ker}\,\varphi \cong \mathrm{Im}\,\varphi$$

が成り立つ．

証 明

$R_1/\mathrm{Ker}\,\varphi$ の任意の元 $\bar{x} = x + \mathrm{Ker}\,\varphi\ (x \in R_1)$ を $(x)\varphi$ に対応させる $R_1/\mathrm{Ker}\,\varphi$ から $\mathrm{Im}\,\varphi$ の上への写像は定義できる．それを $\bar{\varphi}$ とすると，$\bar{\varphi}$ は加法

群としての同型写像である．さらに，R_1 の任意の元 x, y と R_1 の単位元 1 と R_2 の単位元 $1'$ に対して，

$$(\bar{x}\ \bar{y})\,\bar{\varphi} = (\overline{xy})\,\bar{\varphi} = (xy)\,\varphi = (x)\,\varphi\,(y)\,\varphi = (\bar{x})\,\bar{\varphi}(\bar{y})\,\bar{\varphi}$$
$$(\bar{1})\,\bar{\varphi} = (1)\,\varphi = 1'$$

となるので，$\bar{\varphi}$ は環としての同型写像になる．

一般に，環 R の元 a と整数 m に対して，ma を次のように定める．

$$ma = a + a + \cdots + a\ (m\text{ 個の和}) \qquad (m \geqq 0)$$
$$ma = -((-m)\,a) \qquad (m < 0)$$

K を体とするとき，$n1 = 0$ となる自然数 n があれば，その最小の自然数を K の**標数**という．また，そのような自然数がないとき，K の**標数**は 0 であるという．

体 K の部分集合 S に対し，S を含む K の部分体のうちで最小のものを S で**生成**される K の部分体という．それが

$$\bigcap_{M\,:\,S\text{ を含む }K\text{ の部分体}} M$$

と一致することはやさしく分かる．とくに，単位元 1 で生成される K の部分体を K の**素体**という．明らかに，K の素体は K の最小の部分体，すなわち K の任意の部分体に含まれる体である．ここで，

$$\pi = \{m1 \mid m \in \boldsymbol{Z}\}$$

とおくと，π は K の部分整域である．そして，$\boldsymbol{Z}$ の任意の元 m を π の元 $m1$ に対応させる写像 φ は，$\boldsymbol{Z}$ から π の上への環としての準同型写像である．定理 1.8.4 より，

$$\boldsymbol{Z}/\mathrm{Ker}\,\varphi \cong \mathrm{Im}\,\varphi = \pi.$$

したがって，$\mathrm{Ker}\,\varphi = \{0\}$ のときは $\boldsymbol{Z} \cong \pi$ である．このとき，K の素体は有理数体 $\boldsymbol{Q}$ と同型な体となる．一方 $\mathrm{Ker}\,\varphi \neq \{0\}$ のときは，$\mathrm{Ker}\,\varphi$ に含まれる最小の自然数を n とすると，

$$\mathrm{Ker}\,\varphi = \{mn \mid m \in \boldsymbol{Z}\} = n\boldsymbol{Z}$$

となることが分かる．ここで定理 1.8.2 を用いることによって，n は素数であ

り，π は $\boldsymbol{Z}_n$ と同型な体である．

以上をまとめると，次の定理を得る．

定 理 | 1.8.5

体 K の標数が 0 ならば，K の素体は有理数体 $\boldsymbol{Q}$ と同型である．一方，K の標数 n が 0 でないならば，n はある素数 p と等しくなり，K の素体は $\boldsymbol{Z}_p$ と同型である．

定 理 | 1.8.6

K を標数 p の体とし，a, b を K の元とすると，

$$(a+b)^p = a^p + b^p.$$

証 明

$$(a+b)^p = a^p + b^p + \sum_{i=1}^{p-1} \binom{p}{i} a^i b^{p-i}$$

が成り立ち，$\binom{p}{i}$ は p の倍数である $(1 \leqq i \leqq p-1)$．

以下，元の個数が有限個の体である**有限体**について述べるが，証明は省略する（[和；10] 参照）．

定 理 | 1.8.7 **Wedderburn の定理**

元の個数が有限個の斜体は可換体である．

定 理 | 1.8.8

有限体 K の元の個数はある素数の巾であり，乗法群 $K^* = K - \{0\}$ は巡回群である．また，任意の素数 p と任意の自然数 n に対して，元の個数が p^n となる有限体 K は同型なものを除くとただ 1 つ存在する．とくに，K は素体 $\boldsymbol{Z}_p$ 上の n 次元線形空間と見なせる．

元の個数が p^n となる有限体は普通 $GF(p^n)$ で表し，とくに $GF(p)$ は $\boldsymbol{Z}_p$ と同型である．

定　理｜1.8.9

素数 p，自然数 n に対して $q = p^n$ とおくとき，$GF(q)$ の素体 $GF(p)$ の元を係数とする 1 変数 x の n 次既約多項式

$$f(x) = x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots + a_{n-1}x + a_n$$

がある．($f(x)$ は $GF(p)$ の元を係数とする多項式には因数分解できない．)
そして，そのような $f(x)$ は $GF(q)$ において必ず 1 次式の積に分解される．
さらに，a を $GF(q)$ の元で $f(a) = 0$ とすると，$GF(q)$ の各元は

$$b_0 + b_1a + b_2a^2 + \cdots + b_{n-1}a^{n-1} \qquad (b_i \in GF(p))$$

という形に一意的に表される．

有限体の応用例の 1 つとして，次節で直交ラテン方陣について述べよう．後の章で紹介するが，直交ラテン方陣は他の組合せ構造とも深く関係している．

1.9　直交ラテン方陣（ほうじん）

n 個の文字からなる集合 Ω の各文字(成分)を n 回ずつ使って，合計 n^2 個を n 行 n 列の正方形の枡（ます）に配列し，各行各列に文字の重複がないものを **n 次ラテン方陣**という．

例｜1.9.1

すべての自然数 n に対して，n 次ラテン方陣は存在する．実際，第 1 行を 1 段下げるごとに 1 枡右へ動かす配列

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & n-1 & n \\ n & 1 & 2 & \cdots & n-2 & n-1 \\ n-1 & n & 1 & \cdots & n-3 & n-2 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 2 & 3 & 4 & \cdots & n & 1 \end{pmatrix}$$

は n 次テテン方陣である.

さて,

$$\begin{pmatrix} \text{ア} & \text{イ} & \text{ウ} & \text{エ} \\ \text{ウ} & \text{エ} & \text{ア} & \text{イ} \\ \text{エ} & \text{ウ} & \text{イ} & \text{ア} \\ \text{イ} & \text{ア} & \text{エ} & \text{ウ} \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$

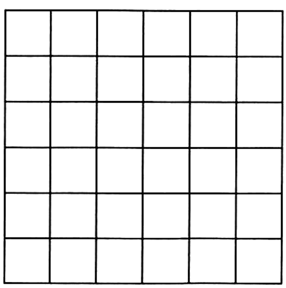
はどちらも 4 次ラテン方陣であり，さらにこの場合，それらの対応する場所にある文字どうしを並べた方陣

$$\begin{pmatrix} \text{ア}1 & \text{イ}2 & \text{ウ}3 & \text{エ}4 \\ \text{ウ}4 & \text{エ}3 & \text{ア}2 & \text{イ}1 \\ \text{エ}2 & \text{ウ}1 & \text{イ}4 & \text{ア}3 \\ \text{イ}3 & \text{ア}4 & \text{エ}1 & \text{ウ}2 \end{pmatrix}$$

には，16 $(= 4\times 4)$ 個の相異なる対が全部現れる．このようなとき，それら 2 つのラテン方陣は**直交**するという．また，一般に 2 つの n 次ラテン方陣の**直交**も同様に定める．

1779 年にオイラーは以下の 36 人士官の問題を出した：ここに第 1 連隊から第 6 連隊まで 6 個の連隊がある．各連隊から 1 級士官，2 級士官，…，6 級士官それぞれ 1 人ずつ選出し，合計 36 人集める．これら 36 人を配置できる 6 行 6 列の正方形の場所に，次の条件をみたすように配置することは不可能ではないか．

出身連隊だけに注目すると，行と列各々の並びには各連隊から 1 人ずつ出ている．また階級だけに注目しても，行と列各々の並びには 1 級から 6 級まで 1



人ずつ出ている．

この36人士官の問題はラテン方陣の表現を使うと，直交する2つの6次ラテン方陣は存在しないのではないか，ということと同値である．この予想が正しいことを最初に証明したのはTarry［論；32］で，1900年のことであった．そして1960年には，$n \neq 2, 6$ ならば直交する2つの n 次ラテン方陣が存在することが証明された（［論；4, 5］参照）．

そこで次に問題になるのは，各自然数 n に対して，互いに直交する n 次ラテン方陣の最大個数 $N(n)$ の決定であろう．上で述べたことをふまえると，

$$N(1) = N(2) = N(6) = 1$$

$$N(n) \geqq 2 \qquad (n \geqq 3,\ \ n \neq 6)$$

である．

定　理｜1.9.2

2以上のすべての整数 n に対して $N(n) \leqq n-1$ が成り立つ．

証　明

いま，$A_1, A_2, \cdots, A_r$ を互いに直交する n 次ラテン方陣とする．ここで，それらの各成分は $\Omega = \{1, 2, \cdots, n\}$ の元としてよく，A_t の i 行 j 列成分を a^t_{ij} とおく $(1 \leqq i, j \leqq n)$．Ω 上の任意の置換 $\pi_1, \pi_2, \cdots, \pi_r$ に対して，$(A_t)\pi_t$ を i 行 j 列成分が $(a^t_{ij})\pi_t$ である n 行 n 列の方陣とすると $(t = 1, 2, \cdots, r)$，$(A_1)\pi_1, (A_2)\pi_2, \cdots, (A_r)\pi_r$ は互いに直交する n 次ラテン方陣であることがやさしく分かる．ところで，$(A_t)\pi_t$ $(t = 1, 2, \cdots, r)$ の第1行はどれも左から $1, 2, \cdots, n$ になるように π_t $(t = 1, 2, \cdots, r)$ をとることができる．そのとき，$(A_1)\pi_1, (A_2)\pi_2, \cdots, (A_r)\pi_r$ の2行1列成分に注目すると，それらはラテン方陣の性質よりどれも1と異なり，さらにそれらは互いに異ならなければならない．なぜならば，任意の $1 \leqq s < t \leqq n$ に対して $(A_s)\pi_s$ と $(A_t)\pi_t$ は直交し，それらの第1行に注目すると，1と1，2と2，3と3，…，n と n の対が現れるからである．したがって，$r \leqq n-1$ でなければならない．

上の定理において等号 $N(n) = n-1$ が成立するとき，互いに直交する $n-1$ 個の n 次ラテン方陣を n 次ラテン方陣の**完全直交系**という．n 次ラテン方陣の完全直交系が存在する n を決定する問題は有名な未解決問題であるが，有限体を用いることによって次の定理を得る．

定理 1.9.3

素数 p と自然数 n に対して $q = p^n$ とおくと，$q \geqq 2$ のとき q 次ラテン方陣の完全直交系は存在する．

証明

q 個の元からなる有限体

$$GF(q) = \{\alpha_1, \alpha_2, \cdots, \alpha_q\}$$

をとり，$\alpha_q = 0$ (零元) とする．q 行 q 列の方陣 $A_1, A_2, \cdots, A_{q-1}$ を，$t = 1, 2, \cdots, q-1$ に対して次のように定める．

$$A_t \text{ の } i \text{ 行 } j \text{ 列成分} = \alpha_i \alpha_t + \alpha_j \qquad (1 \leqq i, j \leqq q)$$

$\alpha_t \neq 0$ なので

$$\{\alpha_1 \alpha_t, \alpha_2 \alpha_t, \cdots, \alpha_q \alpha_t\} = \{\alpha_1, \alpha_2, \cdots, \alpha_q\}$$

が成り立ち，また

$$\{\alpha_1 + \alpha_j, \alpha_2 + \alpha_j, \cdots, \alpha_q + \alpha_j\} = \{\alpha_1, \alpha_2, \cdots, \alpha_q\}$$

$$\{\alpha_i \alpha_t + \alpha_1, \alpha_i \alpha_t + \alpha_2, \cdots, \alpha_i \alpha_t + \alpha_q\} = \{\alpha_1, \alpha_2, \cdots, \alpha_q\}$$

が成り立つ．よって，$A_1, A_2, \cdots, A_{q-1}$ は n 次ラテン方陣である．さらに，A_s と A_t は $s \neq t$ のとき直交する．実際，

$$(\alpha_i \alpha_s + \alpha_j, \alpha_i \alpha_t + \alpha_j) = (\alpha_u \alpha_s + \alpha_v, \alpha_u \alpha_t + \alpha_v)$$

とすると，

$$(\alpha_i - \alpha_u)\alpha_s = \alpha_v - \alpha_j = (\alpha_i - \alpha_u)\alpha_t$$

が成り立つ．ここで $\alpha_s \neq \alpha_t$ なので，$\alpha_i - \alpha_u = 0$ である．したがって $\alpha_i = \alpha_u$ が成り立ち，それゆえ $\alpha_j = \alpha_v$ も成り立つ．

2章 多重可移置換群と組合せゲーム

2.1 置換群に関するいくつかの言葉

本節では，置換群を扱うときによく使われる言葉をまとめて紹介する．

Ω 上の置換群 G が，$t \leqq |\Omega|$ をみたす自然数 t に関して Ω 上 t **重可移**であるとは，Ω の相異なる任意の t 個の元 $\alpha_1, \alpha_2, \cdots, \alpha_t$ と相異なる任意の t 個の元 $\beta_1, \beta_2, \cdots, \beta_t$ に対して，

$$(\alpha_i)g = \beta_i \qquad (i = 1,\ 2,\ \cdots,\ t)$$

をみたす G の元 g があるときにいう．とくに $t = 1$ のとき，G は Ω 上**可移**であるという．また $t \geqq 2$ のとき，G は Ω 上**多重可移**であるという．明らかに，G が Ω 上 t $(\geqq 2)$ 重可移ならば，$1 \leqq k \leqq t$ をみたす任意の整数 k に対して G は Ω 上 k 重可移である．

1981 年に，多くの群論研究者による膨大な成果の結晶として有限単純群分類の完成が宣言された［和；7］．その分類定理を用いると有限次数の多重可移置換群は決定される．だからと言って，多重可移置換群の学習は意味がないということにはならない．本書の主旨である組合せ論の導入として，多重可移置換群より弱い群が作用する組合せ構造の研究方法へのヒントとして，あるいは Appendix で触れるような無限次数多重可移置換群の研究方法として，などの意義がある．さらに，本章の後半で紹介するようなゲームの構造の説明にわざわざ有限単純群の分類定理のような大掛かりな結果を用いては，余りにもアンバランスだということをご理解いただきたい．

そもそも筆者が Miller による定理 1.2.2 の証明が好きなのは，置換に関する定理の証明でわざわざ多項式の一つである差積を使っていないからである．本書と直接の関係はないが，複素数体が代数的閉体であることの証明で関数論を使わない証明が好きなのも同じである．当然，有限単純群の分類定理を使わない有限次多重可移置換群の分類定理もチャレンジすべきであるが，これは相

当難しいことであろう．Appendix で紹介する定理 A. 2 のように，ひょっこりできる可能性はまずない．

ただ，4 章で紹介する定理 4. 3. 5 や定理 4. 5. 5 は群の作用を一切仮定していないものの，有限次多重可移置換群にかなり近いところの結果である．それから想像できることは，多重可移置換群の定義があまりにも“群”に依存したものであり，それを弱めたやや“組合せ論的”な性質で未だ発見されてない重要なものがその問題の解決につながるのではないか，ということである．

例 | 2. 1. 1

$|\Omega| = n$ のとき Ω 上の対称群 S_n は n 重可移であり，$|\Omega| = n \geqq 3$ のとき Ω 上の交代群 A_n は $(n-2)$ 重可移である．

証 明

前半の S_n については明らかである．

後半については，$\alpha_1, \alpha_2, \cdots, \alpha_{n-2}$ と $\beta_1, \beta_2, \cdots, \beta_{n-2}$ をそれぞれ任意の $n-2$ 個の元とし，

$$\Omega - \{\alpha_1, \alpha_2, \cdots, \alpha_{n-2}\} = \{\alpha_{n-1}, \alpha_n\}, \qquad \Omega - \{\beta_1, \beta_2, \cdots, \beta_{n-2}\} = \{\beta_{n-1}, \beta_n\}$$

とおく．このとき，2 つの置換

$$\begin{pmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_{n-2} & \alpha_{n-1} & \alpha_n \\ \beta_1 & \beta_2 & \cdots & \beta_{n-2} & \beta_{n-1} & \beta_n \end{pmatrix}, \qquad \begin{pmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_{n-2} & \alpha_{n-1} & \alpha_n \\ \beta_1 & \beta_2 & \cdots & \beta_{n-2} & \beta_n & \beta_{n-1} \end{pmatrix}$$

のどちらかは偶置換である．

Ω 上の置換群 G が，すべての $\alpha \in \Omega$ に対して $G_\alpha = 1$ をみたすとき，G は Ω 上**半正則**であるという．とくに，Ω 上の半正則置換群 G が Ω 上可移であるとき，G は Ω 上**正則**であるという．

定 理 | 2. 1. 2

G は有限集合 Ω 上半正則な置換群とすると，すべての G-軌道の長さは $|G|$ に等しい．

証明

定理 1.3.2 を用いることによって分かる.

定理 | 2.1.3

Ω 上の可移置換群 G が可換ならば, G は Ω 上正則である.

証明

Ω の任意の元 α, β に対して, $(\alpha)g = \beta$ となる $g \in G$ が存在する. このとき,

$$g^{-1}G_\alpha g = G_\beta$$

である(例 1.4.1 参照). 一方, G は可換群であるから

$$g^{-1}G_\alpha g = G_\alpha$$

である. ここで, β はすべての Ω の元をとることができるので, $G_\alpha = 1$ でなければならない.

例 | 2.1.4

$\Omega = \{1, 2, 3, 4\}$ 上の 2 つの置換群

$$K = \{1,\ (1\ \ 2\ \ 3\ \ 4),\ (1\ \ 3)(2\ \ 4),\ (1\ \ 4\ \ 3\ \ 2)\}$$

$$L = \{1,\ (1\ \ 2)(3\ \ 4),\ (1\ \ 3)(2\ \ 4),\ (1\ \ 4)(2\ \ 3)\}$$

は, どちらも Ω 上正則である.

G を Ω 上の置換群とし, Δ を Ω の部分集合とする. もし, G のすべての元 g に対して

$$\Delta^g \cap \Delta = \Delta \quad \text{または} \quad \Delta^g \cap \Delta = \emptyset$$

が成り立つとき, Δ を G の**ブロック**といい, $|\Delta|$ を Δ の長さという. なお, Δ^g は $(\Delta)g$ のことである. 明らかに Ω 自身あるいは 1 つの元からなる集合 $\{\alpha\}$ ($\alpha \in \Omega$) は G のブロックであり, それらを自明なブロックという.

G を Ω 上の可移置換群とするとき, G が自明でないブロックをもつならば G を**非原始置換群**といい, 自明でないブロックをもたないならば G を**原始置

換群という．

定　理｜2.1.5

G を有限集合 Ω 上の非原始置換群とし，Δ を G の自明でないブロックとすると，G のブロック $\Delta=\Delta^{x_1},\Delta^{x_2},\cdots,\Delta^{x_m}$ があって $(x_i\in G)$，

$$\Omega=\Delta^{x_1}\cup\Delta^{x_2}\cup\cdots\cup\Delta^{x_m}\qquad(\text{直和})$$

と表せる．とくに $|\Delta|$ は $|\Omega|$ の約数である．

証　明

G は Ω 上可移であるから

$$\Omega=\bigcup_{g\in G}\Delta^g$$

が成り立つ．また，G の元 g,h に対して $\Delta^g\cap\Delta^h\neq\emptyset$ とすると，$\Delta^{gh^{-1}}\cap\Delta\neq\emptyset$ となるので，$\Delta^{gh^{-1}}=\Delta$ でなければならない．すなわち，$\Delta^g=\Delta^h$ である．したがって，G に $m=|\Omega|/|\Delta|$ 個の適当な元 $x_1,x_2,\cdots,x_m$ があって，Ω は $\Delta=\Delta^{x_1},\Delta^{x_2},\cdots,\Delta^{x_m}$ の直和として表せる．

定理2.1.5におけるブロックの集合 $\{\Delta=\Delta^{x_1},\Delta^{x_2},\cdots,\Delta^{x_m}\}$ を，Δ を含む G の**非原始系**という．

定　理｜2.1.6

（1）　2重可移置換群は原始置換群である．

（2）　素数次数の可移置換群は原始置換群である．

証　明

（1）　G を Ω 上の2重可移置換群とし，Δ を $|\Delta|\geqq 2$ をみたす Ω の真部分集合とする．G は Ω 上2重可移であるから，Δ の異なる2元 α,β と $\Omega-\Delta$ の元 γ に対して，

$$(\alpha)g=\alpha,\qquad(\beta)g=\gamma$$

となる G の元 g が存在する．よって

$$\varDelta^g \cap \varDelta \neq \emptyset, \quad \varDelta^g \neq \varDelta$$

が成り立つので，$\varDelta$ はブロックではない．

（2） 定理 2.1.5 より明らかである．

例 2.1.7

G を次のように定める $\Omega = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ 上の置換群とすると，G は位数 81 の非原始置換群となり，$\{\{1, 2, 3\}, \{4, 5, 6\}, \{7, 8, 9\}\}$ は G の非原始系となる．

$$G = \langle a, b, c, d \rangle,$$
$$a = (1 \quad 2 \quad 3), \quad b = (4 \quad 5 \quad 6), \quad c = (7 \quad 8 \quad 9),$$
$$d = (1 \quad 4 \quad 7)(2 \quad 5 \quad 8)(3 \quad 6 \quad 9).$$

実際，$\{\{1, 2, 3\}, \{4, 5, 6\}, \{7, 8, 9\}\}$ が G の非原始系であることは明らかで，また G は位数 27 の正規部分群 $\langle a, b, c \rangle$ と位数 3 の部分群 $\langle d \rangle$ の半直積である．

2.2 多重可移置換群

最初に，1.3 節で定義した固定部分群を一般化して定義する．集合 Ω 上の置換群 G と Ω の部分集合 $\varDelta$ に対して，

$$G_\varDelta = \{g \in G \mid \text{すべての } \alpha \in \varDelta \text{ に対して } (\alpha)g = \alpha\},$$
$$G_{(\varDelta)} = \{g \in G \mid (\varDelta)g = \varDelta\}$$

とおくと，それらは G の部分群である．前者を G における $\varDelta$ の(点ごとの)**固定部分群**といい，後者を G における $\varDelta$ の**集合としての固定部分群**という．とくに $\varDelta = \{\alpha_1, \alpha_2, \cdots, \alpha_t\}$ のとき，$G_\varDelta$ を $G_{\alpha_1\alpha_2\cdots\alpha_t}$ あるいは $G_{\alpha_1, \alpha_2, \cdots, \alpha_t}$ で表すこともよくある．次の 2 つの定理が成り立つことはやさしく分かる(定理 2.2.2 については例 1.4.1 を参照)．

定　理 2.2.1

k, t を $1 \leqq k < t$ をみたす自然数とし，G を Ω 上の k 重可移置換群とする．

$|\Delta| = k$ をみたす Ω のある部分集合 Δ に関して，G_Δ を $\Omega-\Delta$ 上の置換群と見なすと $(t-k)$ 重可移ならば，G は Ω 上 t 重可移である．

定　理 | 2.2.2

G を Ω 上の t 重可移置換群とし，Γ, Δ を t 個の元からなる Ω の部分集合とする．このとき，

$$G_\Delta = g^{-1}G_\Gamma g$$

となる G の元 g が存在する．

次の定理は，定理 1.3.2 をくり返し用いることによって直ちに導かれる．

定　理 | 2.2.3

G を Ω 上の t 重可移置換群，Δ を t 個の元からなる Ω の部分集合，$|\Omega| = n$ とするとき，

$$|G| = n(n-1)\cdots(n-t+2)(n-t+1)|G_\Delta|$$

が成り立つ．

多重可移置換群を扱うとき，次の Jordan-Witt の定理は大変重要であり，有限次数の場合ばかりでなく無限次数の場合にも適用できるものである．それを紹介する前に，いくつかの必要な定義を述べる．

Ω 上の置換群 G の元 g と部分集合 H は，Ω の部分集合 Δ を集合として固定しているとする．すなわち，$(\Delta)g = \Delta$ であり，$(\Delta)h = \Delta$ がすべての $h \in H$ について成り立つ．このとき，H および g の Δ への制限をそれぞれ H^Δ, g^Δ で表す．

次に，Ω 上の置換群 G の元 g と部分集合 H に対して，

$$I(g) = \{\alpha \in \Omega \mid (\alpha)g = \alpha\}.$$

$$I(H) = \{\alpha \in \Omega \mid \text{すべての } h \in H \text{ に対して } (\alpha)h = \alpha\}$$

と定め，それらを g あるいは H の**固定点集合**という．

定　理 | 2.2.4 ……………………………………Jordan-Witt

G を Ω 上の t 重可移置換群，$\Delta=\{\delta_1, \delta_2, \cdots, \delta_t\}$ を t 個の元からなる Ω の部分集合とし，H は次の条件をみたす G_Δ の部分群とする：H と G-共役な G_Δ の部分群は H と必ず G_Δ-共役である．このとき，G における H の正規化群 $N_G(H)$ を $I(H)$ 上に制限した置換群 $N_G(H)^{I(H)}$ は $I(H)$ 上 t 重可移となる．

証　明 ……………………………………

最初に，$N_G(H)$ は $I(H)$ を集合として固定する．実際，$N_G(H)$ の任意の元 g と $I(H)$ の任意の元 α をとると，H の任意の元 h に対して $gh=kg$ となる $k\in H$ があり，

$$(\alpha^g)^h=\alpha^{gh}=\alpha^{kg}=\alpha^g$$

となるので，$(\alpha)g=\alpha^g$ は $I(H)$ の元である．よって，$I(H)^g\subseteqq I(H)$ が成り立つが，

$$I(H)=I(H)^{g^{-1}g}\subseteqq I(H)^g\subseteqq I(H)$$

となるので，$I(H)^g=I(H)$ が成り立つ．

以下，$I(H)$ の相異なる任意の元 $\alpha_1, \alpha_2, \cdots, \alpha_t$ に対して，$(\alpha_i)g=\delta_i\ (i=1, 2, \cdots, t)$ となる $g\in N_G(H)$ があることを示せばよい．まず，G は Ω 上 t 重可移であるから，$(\alpha_i)x=\delta_i\ (i=1, 2, \cdots, t)$ となる $x\in G$ は存在する．ここで，

$$I(x^{-1}Hx)=I(H)^x\supseteqq\{\alpha_1, \alpha_2, \cdots, \alpha_t\}^x=\{\delta_1, \delta_2, \cdots, \delta_t\}$$

となるから，$x^{-1}Hx$ は G_Δ の部分群である．そこで仮定を使って，ある $y\in G_\Delta$ があって，

$$x^{-1}Hx=y^{-1}Hy$$

となる．よって，xy^{-1} は $N_G(H)$ の元であり，さらに

$$(\alpha_i)xy^{-1}=(\delta_i)y^{-1}=\delta_i \qquad (i=1, 2, \cdots, t)$$

をみたす．よって，$g=xy^{-1}$ とおけばよい．

本章の後半では本質が置換群と見なすことができるいくつかのゲームを扱うが，そこで用いる1800年代後半に得られた3つの定理を，証明を省略して述べ

よう．なお定理 2.2.5 に関しては，1954 年に M. Hall によって一般化した定理を，無限次数多重可移置換群の研究と関連させて最後の章で述べる．

定　理 | 2.2.5 ……Jordan [論；19]

G を有限集合 Ω 上の 4 重可移置換群とし，Ω の相異なる 4 つの元 $\alpha, \beta, \gamma, \delta$ に対して $G_{\alpha\beta\gamma\delta}=1$ とする．このとき，G は S_4, S_5, A_6 または M_{11} のどれかと(置換群としての同型を除いて)一致する．

上の定理において，S_4, S_5 はそれぞれ 4 次，5 次の対称群，A_6 は 6 次の交代群，そして M_{11} は 11 文字上のマシュー群というものである(位数は $11\cdot10\cdot9\cdot8$)．M_{11} については次の章で他のマシュー群も含めて置換群的な構成を紹介する．

定　理 | 2.2.6 ……Marggraf [論；24]

次数 n の原始置換群 G が $1<m<n$ をみたす長さ m の巡回置換を含むならば，G は $(n-m+1)$ 重可移置換群となる．

定　理 | 2.2.7 ……Bochert [論；3]

G を n 個の元からなる集合 Ω 上の原始置換群とし，$G\neq A^\Omega, S^\Omega$ とする．このとき，

$$|S^\Omega : G| \geqq \left[\frac{n+1}{2}\right]!$$

が成り立つ．ただし，$[x]$ は x を超えない最大の整数を意味する．

2.3　15 ゲームと新 15 ゲーム

古くから親しまれてきた**15 ゲーム**は，1 から 15 までの数字が書いてある 15 個の同一正方形の小パネルを，それらがぴったり 16 個分入る正方形の枠に入れ，空白部分に小パネルを次々と動かして基本形に並べ換えるゲームである．体験的によく知られているように，そのゲームには完成するものとしないもの

9	5	11	4
7	10	8	2
14	13	6	12
15	1	3	

⇨ 完成

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

基本形

9	5	10	3
15	1	2	14
12	13	8	4
7	11	6	

⇨ 完成しない

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

基本形

がある(上図参照)．本節では，その 15 ゲームとそれを筆者が難しく改良した新 15 ゲームについて置換群の立場から解説する．

最初に，空白は 16 が付いている小パネルと見なすと，15 ゲームは $\bar{\Omega}=\{1, 2, \cdots, 16\}$ 上の置換に関するゲームと見なせるのである．そして 1 回の操作は，16 が付いているパネルとその上下左右にあるパネルとの互換である．さらに，右下の部分に空白(16 が付いているパネル)がある状態がゲームの開始と終了の位置であることに注目すると，15 ゲームは $\Omega=\{1, 2, \cdots, 15\}$ 上の置換に関するゲームとも見なせる．

さて，16 が付いているパネルはゲームの開始時と終了時は右下にあるので，途中の過程ですぐ上のパネルとそれを交換した回数とすぐ下のパネルとそれを交換した回数は等しく，途中の過程ですぐ左のパネルとそれを交換した回数とすぐ右のパネルとそれを交換した回数は等しい．したがって，ゲームの開始から終了まで，互換が作用した回数は偶数回である．よって，

$$A^{\bar{\Omega}} \cap S^{\Omega} = A^{\Omega}$$

であることに注目すれば，基本形と偶置換の関係になっている状態から開始しないと，ゲームは完成できないのである．

逆に，基本形と偶置換の関係になっている状態から開始すると，ゲームは必ず完成できることを示そう．まず各 $i=1, 2, \cdots, 15$ について，基本形で i が付いているパネルが置かれている場所を 15 ゲームにおける i という場所とする．

そして，15ゲームの**自己同型群** G を次のように定める．

$G=\{\sigma\in A_{15}|$ 場所 $i\ (i=1,2,\cdots,15)$ にあるパネルを場所 $(i)\sigma$ に一緒に移す変形はできる$\}$

たとえば，変形

α_1	α_2	α_3	α_4
α_5	α_6	α_7	α_8
α_9	α_{10}	α_{11}	α_{12}
α_{13}	α_{14}	α_{15}	

$\Rightarrow$

α_{14}	α_8	α_{15}	α_4
α_2	α_{11}	α_5	α_7
α_1	α_6	α_3	α_{12}
α_{10}	α_9	α_{13}	

はできるので，

$$\sigma=\begin{pmatrix}1&2&3&4&5&6&7&8&9&10&11&12&13&14&15\\9&5&11&4&7&10&8&2&14&13&6&12&15&1&3\end{pmatrix}$$

は G の元である．

定　理 | 2. 3. 1

15ゲームの自己同型群 G は Ω 上の交代群 A_{15} と一致する．

証　明

Ω の相異なる任意の2元 i,j に対して，

$(1)\sigma=i,\qquad(2)\sigma=j$

となる元 σ が G に存在することはやさしく分かる．したがって G は Ω 上2重可移であり，定理2. 1. 6 (1) より G は Ω 上の原始置換群となる．また，変形

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

$\Rightarrow$

1	2	3	4
5	6	7	8
9	10	12	15
13	14	11	

は太い線の枠の中だけ動かしてできる．したがって，G は長さ3の巡回置換を含む．そこで定理2. 2. 6，定理2. 2. 3 および定理2. 2. 7 を使うと，$G=A_{15}$ を

得る.

定理 2.3.1 より，15 ゲームでは完成するものとしないものがちょうど半々であることが分かる.

さて筆者は，「15 ゲームではやさしくてつまらない」と思う方々を対象にして，少し難しくした新 15 ゲームを 1999 年に考案した．そして，それをインターネット上で無料で遊べるように城西大学の山崎正之氏に公開していただき，「New 15 Puzzle by Mitsuo Yoshizawa」と入力すると誰でも気軽に楽しめるようになっている.

その新 15 ゲームは，以下のように左から右へ変形していくものであって，灰色部分は小パネルを入れられない場所である.

実は新 15 ゲームも，最初に 15 枚の小パネルをばらばらに取り出すと，完成するものとしないものはちょうど半々である．それを示すために，Ω と自己同型群 G を 15 ゲームと同様に定めて，次の定理を証明すればよい.

α_2	α_3	α_4	α_5
α_1			α_6
α_9	α_8	α_7	
α_{10}			α_{15}
α_{11}	α_{12}	α_{13}	α_{14}

⇨

2	3	4	5
1			6
9	8	7	
10			15
11	12	13	14

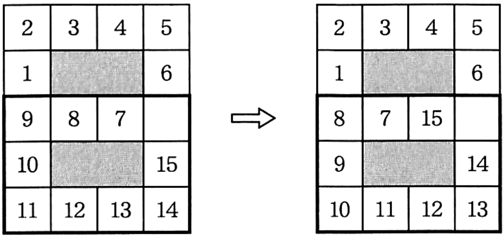
基本形

定 理 | 2.3.2

新 15 ゲームの自己同型群 G も Ω 上の交代群 A_{15} と一致する.

証 明

$G \leqq A_{15}$ であることは 15 ゲームの場合と同様にして分かる．また，G が Ω 上 2 重可移であり，それゆえ原始置換群であることもやさしく分かる．さらに，変形



は太い線の枠の中だけ動かしてできる．したがって，G は長さ 9 の巡回置換を含む．そこで定理 2.2.6 を使うと，G は Ω 上 7 重可移である．そして定理 2.2.3 と定理 2.2.7 を適用すると，もし $G \neq A_{15}$ ならば G における $\{1, 2, 3, 4, 5, 6, 7\}$ の(点ごとの)固定部分群 $G_{1234567}$ は単位群 1 になることが分かる．ここで，$(G_{123})^{\Omega-\{1,2,3\}}$ は $\Omega-\{1, 2, 3\}$ 上の 4 重可移置換群なので，定理 2.2.5 より

$$|\Omega|-3 = 4, 5, 6 \text{ または } 11$$

となって矛盾である．

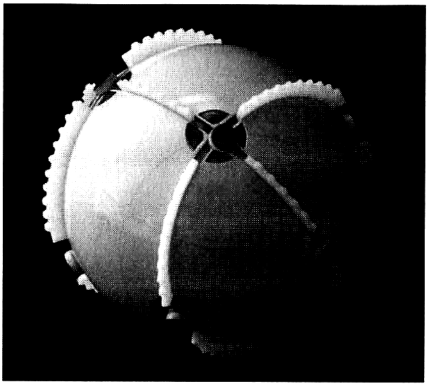
なお，古くは [論；31] などで 20 次以下の原始置換群は表になっており，最近では 1000 次以下の原始置換群も本質的に表になっている([洋；12] 参照)．それゆえ，上記の証明は置換群の歴史を学ぶつもりで理解するとよいのかもしれない．このことに関しては，次節でも同じことがいえる．

最後に新 15 ゲームの 1 つの原理的な解法を大まかに述べると，まず 7 と 8 が付いているパネルを基本形の位置に移動する．次に，基本形で 1 と 2 の場所にある小パネルどうしの互換と 7 と 8 の場所にある小パネルどうしの互換の合成として表せる置換 σ はゲームの移動としてやさしくできることに注目する．そして，外周の小パネルを 1 つずつ回すように動かす長さ 13 の巡回置換 τ と σ を組み合わせることにより，外周上にある 13 個の小パネルを基本形に移すことができる．

2.4 球面上のあるゲーム

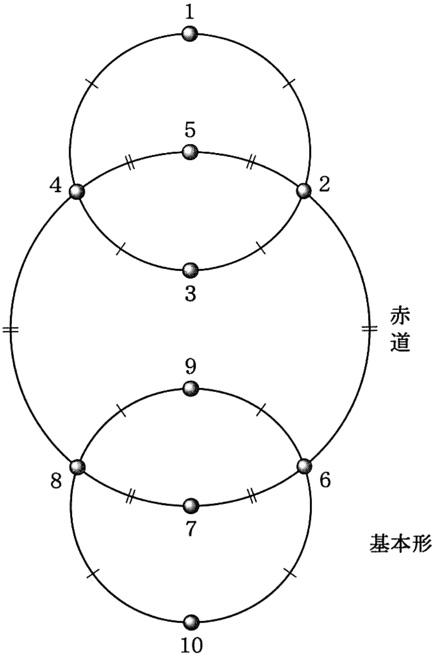
本質が置換群のゲームはいろいろあるが，難易度，操作性，価格などの面でどれも一長一短であろう．2001 年に筆者は，置換の合成を実感させる目的で次の写真にある知育玩具の試作品を完成させた．以後，それをマジック S 10 とよ

ぶことにする．21 世紀の日本を支える子供達のために日本のおもちゃメーカーに製品化していただきたいと願っているものの，相談を受けるのは海外の方々ばかりで残念である．なお，マジック S 10 に関しても前節の新 15 ゲームと同様に，金銭的な権利は一切求めるつもりがない．本節ではマジック S 10 の置換群的な特徴付けを行い，さらにはそれを一般化したゲームの置換群的な特徴付けも行う．



マジック S 10

マジック S 10 は，球面体の赤道に溝を設け，それに沿って 6 個の小球を等間隔に埋め，小球どうしの間に赤道に沿った回転を補助する 6 個の同じサイズの小片をぴったりはめる．次に球面上で，赤道に直交する同じ半径の 2 つの円周に沿って溝を設ける．ただし，それらは平行で，それらの球面上の距離は先に埋めた隣どうしの小球の球面上における距離とする．そして，新たに設けた 2 つの円周に沿った溝では，それぞれ 2 個の新しい小球と 4 個の同じサイズの小片を入れて回転できるようにする．小球は合計で 10 個になるが，形は同じであるものの互いに異なる 10 色を塗り分ける．また小球と小球の間の小片は，赤道上のものと赤道上にはないものの 2 種類だけである．そして，溝と溝が交叉するところに小球を必ず置くようにして，10 個の小球に関する基本形としてのホームポジションを，印などを付けて定めておく．そのように定めたゲームは，結局次の図で示した置換群のゲームと見なせる．なお，$\partial(i,j)$ は小球 i と小球 j の球面上での距離である．



$$\partial(1,2) = \partial(2,3) = \partial(3,4) = \partial(4,1)$$
$$= \partial(9,6) = \partial(6,10) = \partial(10,8) = \partial(8,9),$$
$$\partial(5,2) = \partial(2,6) = \partial(6,7) = \partial(7,8) = \partial(8,4) = \partial(4,5).$$

以上から，マジック S 10 は $\Omega = \{1, 2, \cdots, 10\}$ 上の置換群 $G = \langle a, b, c\rangle$ のゲームである．ただし，

$$a = (1\quad 2\quad 3\quad 4), \qquad b = (2\quad 6\quad 7\quad 8\quad 4\quad 5),$$
$$c = (6\quad 10\quad 8\quad 9).$$

遊び方は，a, b, c に対応した球面上の操作によって，各小球の位置をばらばらにしておき，最後に基本形に戻すのである．

定　理 | 2.4.1

$G = S_{10}$ である．

証 明

任意の異なる2つの小球 x と y を基本形で1と3のある場所にそれぞれ移すことはやさしくできるので，G は Ω 上2重可移である．よって G は原始置換群であり，定理2.2.6を使うと G は7重可移であることが分かる．したがって，定理2.2.3と定理2.2.7より G は A_{10} または S_{10} となる．そして a は奇置換であるから，$G = S_{10}$ を得る．

ここで，マジックS10の解法を述べよう．最初に，基本形の1, 3, 9, 10の場所に4個の小球を正しく戻す移動はやさしくできる．したがって，赤道上の6個の小球を，それ以外の小球はそのままの場所に置くという条件を付けて，どのような順列にも並べ換えられる移動があることを示せばよい．そのためには，基本形の状態から4と5だけの取り換えを意味する互換(4　5)を作ることができればよい．実際，(4　5)に対応する操作と赤道に沿った回転を組み合わせれば，赤道上の6個の小球はどのような順列にも並べ換えられる(定理1.1.2参照)．

筆者は直観に頼って，

$$(4\quad 5) = a^3bab^2ab^2aba$$

を得た(本書では写像の合成を左から行うことに注意)．これは，ゲームとしては9回の回転操作であるが，その9回は最小回数であることを平成14年度4年ゼミナール生の郡山真君がパソコンを使って確認した．

次に，マジックS10を一般化することを考えよう．まず，上定理の証明あるいは次の定理の結論からも分かるように，共有点をもつ2つの円周が球面上にある場合に限定して一般化することが本質であって，3つ以上の円周の場合は次々とつないで考えればよいのである．

そこで，1つの円周上に $\alpha_1, \alpha_2, \cdots, \alpha_m$ があり，もう1つの円周上に $\beta_1, \beta_2, \cdots, \beta_n$ があると見なして，$\Omega = \{\alpha_1, \alpha_2, \cdots, \alpha_m\} \cup \{\beta_1, \beta_2, \cdots, \beta_n\}$ 上の置換群

$$G = \langle a, b \rangle$$

を決定する問題を考えることにする．ただし，

$$m \leqq n, \quad a = (\alpha_1, \alpha_2, \cdots, \alpha_m), \quad b = (\beta_1, \beta_2, \cdots, \beta_n)$$

として，以下のように4つの場合に分ける．

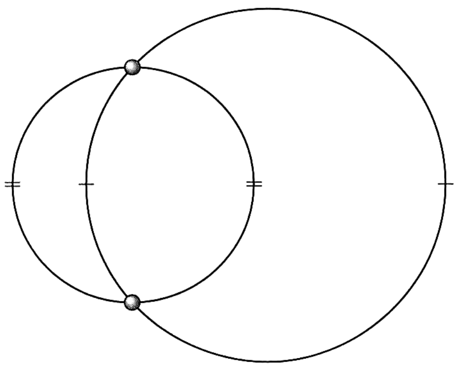
$$\text{I}: m = 2, \quad |\Omega| = \begin{cases} n+1 & (\alpha_1 = \beta_1) \\ \quad \text{または} & \\ n & (\alpha_1 = \beta_1,\ \alpha_2 = \beta_i\,(1 < i \leqq n)). \end{cases}$$

$$\text{II}: m \geqq 3,\ \alpha_1 = \beta_1, \quad |\Omega| = m+n-1.$$

$$\text{III}: m \geqq 3,\ \alpha_1 = \beta_1,\ \alpha_i = \beta_j\,(1 < i \leqq m,\ 1 < j \leqq n),$$
$$|\Omega| = m+n-2,\ m = 2(i-1),\ n = 2(j-1).$$

$$\text{IV}: m \geqq 3,\ \alpha_1 = \beta_1,\ \alpha_i = \beta_j\,(1 < i \leqq m,\ 1 < j \leqq n),$$
$$|\Omega| = m+n-2, \quad \text{III以外の場合}.$$

ここで，たとえばIIIは球面上のゲームとして考えると，下図のように2つの円周の交点がそれぞれの直径の位置関係になっている場合である．



定 理 | 2.4.2

（1） Iの場合，$G = S^{\Omega}$ であるか，G は長さ t のブロックからなる非原始系 $\Pi = \{\Gamma_1, \Gamma_2, \cdots, \Gamma_s\}\left(s = \dfrac{n}{t}\right)$ をもつ非原始置換群で，Π 上の G の作用全体は位数 s の巡回群となる．ただし t は，n と $i-1$ が互いに素でないとき，n を $(n, i-1)$ で割った商である．

（2） IIの場合，$G = S^{\Omega}$ または A^{Ω} となる．

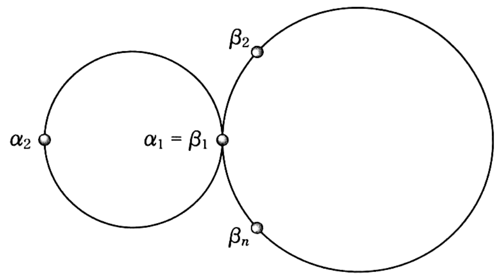
（3） IIIの場合，G は長さ2のブロックからなる非原始系 $\Pi = \{\Gamma_1, \Gamma_2, \cdots,$

$\Gamma_s\}\left(s=\dfrac{m+n-2}{2}\right)$をもつ非原始置換群で，$\Pi$ 上の G の作用全体は対称群 S^{Π} または交代群 A^{Π} となる．

（4）　Ⅳの場合，$G=S^{\Omega}$，A^{Ω} または $PGL(2,5)$ となる．（$PGL(2,5)$ は次章で説明するが，6 文字上の 3 重可移置換群(位数は 6・5・4)で，5 次対称群 S_5 と群として同型なものである.）

証　明

（1）　$|\Omega|=n+1\,(\alpha_1=\beta_1)$ のとき，

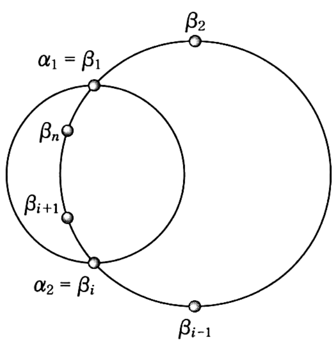


G は Ω 上 2 重可移である．そこで，Ω の任意の 2 元 γ,δ に対して，$(\alpha_1)g=\gamma$，$(\alpha_2)g=\delta$ となる $g\in G$ が存在する．よって，

$$g^{-1}(\alpha_1\quad\alpha_2)g=(\gamma\quad\delta)$$

となるから，G は Ω 上のすべての互換を含む．したがって，$G=S^{\Omega}$ を得る．

次に，$|\Omega|=n\,(\alpha_1=\beta_1,\ \alpha_2=\beta_i\,(1<i\leqq n))$ の場合を考える．



もし$\varDelta$が$\alpha_1=\beta_1$を含む長さ2以上のブロックとすると，$\alpha_2=\beta_i$も$\varDelta$の元でなくてはならない．さらに，nと$i-1$の最大公約数をdとすると，

$$\varDelta=\{\beta_1,\beta_{1+d},\beta_{1+2d},\cdots\}$$

が成り立つことがやさしく分かる(添字はnで割った余り)．もし$d=1$，したがってGが原始置換群ならば，定理2.2.6より$G=S^{\Omega}$である．そしてもし$d>1$ならば，Gは非原始系

$$\varPi=\{(\varDelta)b^j\,|\,j=0,1,\cdots,d-1\}$$

をもつ非原始置換群である．

(2) GがΩ上2重可移であることはやさしく分かる．よってGは原始置換群であり，定理2.2.6を使うとGはΩ上n重可移である．もし$G\neq S^{\Omega}$, A^{Ω}とすると，定理2.2.3，定理2.2.7および$m\leqq n$であることを使うと，

$$(m-1)!\geqq|S^{\Omega}:G|\geqq\left[\frac{m+n}{2}\right]!\geqq m!$$

となって矛盾である．

(3) 球面上のゲームとして考えたとき，両方の円周で直径の位置関係になる2元の集合全体を$\varGamma_1=\{\gamma_1,\delta_1\}$，$\varGamma_2=\{\gamma_2,\delta_2\}$，…，$\varGamma_s=\{\gamma_s,\delta_s\}$ $\left(s=\dfrac{m+n-2}{2}\right)$とする．明らかに$G$は，それらを非原始系とする非原始置換群である．$G$の$\varPi=\{\varGamma_1,\varGamma_2,\cdots,\varGamma_s\}$上の作用全体を考えると，$\varPi$を(1)あるいは(2)における$\Omega$と見なすことによって，(1)と(2)の結論から$G$の$\varPi$上の作用全体は$S^{\varPi}$または$A^{\varPi}$となる．

(4) $m<n$の場合は(2)と同様に証明して，$G=S^{\Omega}$またはA^{Ω}が分かる．$m=n$の場合も(2)と同様に証明して，もし$G\neq S^{\Omega}$, A^{Ω}ならばGはΩ上の$(m-1)$重可移置換群で，

$$|G_{\alpha_1,\alpha_2,\cdots,\alpha_{m-1}}|=1$$

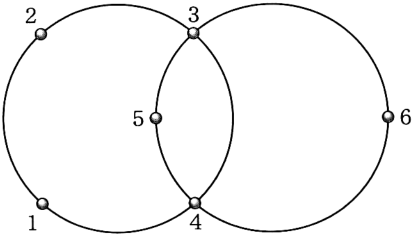
であることが分かる．そしてこのとき，以下mの値を3つの場合に分けて考えることにする．

$m=3$のとき，GがA_4になることは具体的にすぐ分かる．

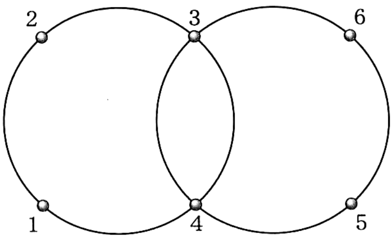
$m\geqq5$かつ$G\neq S^{\Omega}$, A^{Ω}のとき，Gは$m-1\,(\geqq4)$重可移置換群なので，定理2.2.5を使うとこの場合は起こらないことがやさしく分かる．

$m=4$ かつ $G \neq S_6$, A_6 のとき，IIIの場合でないことに留意すると，本質的には次の 2 つの場合(ア)，(イ)に分かれる．

(ア)　$a=(1\quad 2\quad 3\quad 4)$，　$b=(3\quad 5\quad 4\quad 6)$．



(イ)　$a=(1\quad 2\quad 3\quad 4)$，　$b=(3\quad 4\quad 5\quad 6)$．



(ア)のとき，

$$a^2=(1\quad 3)(2\quad 4),$$

$$a^2ba^2=(1\quad 5\quad 2\quad 6).$$

ここで $c=(a^2ba^2)^2=(1\quad 2)(5\quad 6)$ とおくと，

$$c^{-1}ac=(2\quad 1\quad 3\quad 4),$$

$$ac^{-1}ac=(1)(2\quad 4\quad 3)\in G$$

となる．したがって，$G=S_6$ または A_6 となるが，G は奇置換を含むので $G=S_6$ を得る．

(イ)のとき，G は Ω 上 2 重可移で長さ 4 の巡回置換を含むので，G は 6 文字上の 3 重可移置換群となる．そして G は奇置換を含むので，G は S_6 または $PGL(2,5)$ となり，$PGL(2,5)$ は次の群と置換同型である（[論；31] 参照）．

$$\langle d=(1\quad 2\quad 3\quad 4\quad 5),\ e=(2\quad 3\quad 5\quad 4),\ f=(1\quad 6)(3\quad 4)\rangle$$

いま，

$$f^{-1}df = (6\quad 2\quad 4\quad 3\quad 5)$$
$$ef^{-1}df = (2\quad 5\quad 3\quad 6) = (6\quad 2\quad 5\quad 3)$$
$$d^{-1}ed = (3\quad 4\quad 1\quad 5) = (5\quad 3\quad 4\quad 1)$$

なので，

$$x = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 2 & 4 & 5 & 3 & 1 \end{pmatrix}$$

とおけば，

$$x^{-1}(ef^{-1}df)\,x = (1\quad 2\quad 3\quad 4) = a$$
$$x^{-1}(d^{-1}ed)\,x = (3\quad 4\quad 5\quad 6) = b$$

となる．よって，

$$PGL(2,5) \geqq G = \langle a, b\rangle \geqq PGL(2,5)$$

となるので，$G = PGL(2,5)$ を得る．

3章 射影線形群とマシュー群

3.1 射影線形群

一般の体 K の元を成分とする n 次正則行列全体も，$GL(n, \boldsymbol{R})$ と同じように積に関して群となる．これを $GL(n, K)$ と書いて，K 上の n 次**一般線形群**という．また，$GL(n, K)$ の元 A で $\det A = 1$ をみたすもの全体も，$SL(n, \boldsymbol{R})$ と同じように $GL(n, K)$ の正規部分群となる．これを $SL(n, K)$ と書いて，K 上の n 次**特殊線形群**という．例 1.5.5 と同様にして，群として

$$GL(n, K)/SL(n, K) \cong K^* = K - \{0\}$$

が成り立つ．ここで，K が元の個数 q の有限体 $GF(q)$ であるとき，$GL(n, K)$，$SL(n, K)$ をそれぞれ $GL(n, q)$，$SL(n, q)$ で表す．

本来ならば，$GL(n, K)$ を含む一般半線形群 $\Gamma L(n, K)$ をも紹介すべきかもしれないが，本書では扱わないことにする([和；9] 参照)．

次の定理は例 1.4.3 と同様にして得られる．

定理 3.1.1

K を体，I を $GL(n, K)$ における n 次単位行列とすると，

$$Z(GL(n, K)) = \{aI \mid a \in K,\ a \neq 0\}$$
$$Z(SL(n, K)) = SL(n, K) \cap Z(GL(n, K)).$$

$GL(n, K)$ の $Z(GL(n, K))$ による剰余群を $PGL(n, K)$ で表し，$SL(n, K)$ の $Z(SL(n, K))$ による剰余群を $PSL(n, K)$ で表し，それぞれ n 次**射影一般線形群**，n 次**射影特殊線形群**という．ここで，K が有限体 $GF(q)$ であるとき，$PGL(n, K)$，$PSL(n, K)$ をそれぞれ $PGL(n, q)$，$PSL(n, q)$ で表す．

定理 1.5.4 より

$$PSL(n, K) \cong SL(n, K) \cdot Z(GL(n, K))/Z(GL(n, K))$$

であるから，この同型対応により $PSL(n, K)$ は $PGL(n, K)$ の部分群である

と見なせる．さらに

$$GL(n,K)/Z(GL(n,K) \trianglerighteq SL(n,K)\cdot Z(GL(n,K)/Z(GL(n,K))$$

であるから，$PSL(n,K)$ は $PGL(n,K)$ の正規部分群であると見なせる．

なお，$n \geqq 3$ のとき $PSL(n,q)$ は単純群であり，$q \neq 2,3$ のとき $PSL(2,q)$ は単純群であることが知られている（[和；4] 参照）．

定　理 | 3.1.2

$$|GL(n,q)| = (q^n-1)(q^n-q)\cdots(q^n-q^{n-1})$$
$$|SL(n,q)| = (q^n-1)(q^n-q)\cdots(q^n-q^{n-2})\,q^{n-1}$$

証　明

V を $GF(q)$ 上 n 次行ベクトル全体からなる線形空間とする．$\boldsymbol{R}$ や $\boldsymbol{C}$ 上の線数代数学で学んだことと同様にして，$GL(n,q)$ の各行列 A は互いに一次独立な n 個の V の元 $v_1, v_2, \cdots, v_n$ からなる．ただし，v_i は A の第 i 行である．ここで，v_1 の定め方は $q^n-1\,(=|V-\{\mathbf{0}\}|)$ 通り，その各々に対して v_2 の定め方は $q^n-q\,(=|V-\langle v_1\rangle|)$ 通り，それらの各々に対して v_3 の定め方は q^n-q^2 $(=|V-\langle v_1, v_2\rangle|)$ 通りある．以下同様．なお，$\mathbf{0}$ は V の零ベクトル，$\langle v_1\rangle$ は v_1 で生成された V の部分空間，$\langle v_1, v_2\rangle$ は v_1 と v_2 で生成された V の部分空間である．以上から，$GL(n,q)$ の位数に関する公式を得る．

$SL(n,q)$ の位数については，

$$GL(n,q)/SL(n,q) \cong GF(q)^*$$

を使うことにより分かる．

定　理 | 3.1.3

$$|PGL(n,q)| = |GL(n,q)|/(q-1)$$
$$|PSL(n,q)| = |SL(n,q)|/(n,q-1)$$

証　明

$$|Z(GL(n,q))| = q-1$$

であるので，上の等式の成立は明らか．

下の等式については，$d=(n, q-1)$ とおいて，

$$|SL(n,q)\cap Z(GL(n,q))| = d$$

を示せばよい．定理 1.8.8 より，乗法群 $GF(q)^*$ はある元 ω で生成される巡回群 $\langle\omega\rangle$ である．いま，$q-1=df$ とおくと，n 次行列

$$A=\begin{pmatrix} \omega^f & & & O \\ & \omega^f & & \\ & & \ddots & \\ O & & & \omega^f \end{pmatrix}$$

は $SL(n,q)$ における位数 d の元である．逆に，$Z(GL(n,q))$ の元

$$X=\begin{pmatrix} x & & & O \\ & x & & \\ & & \ddots & \\ O & & & x \end{pmatrix}$$

が $SL(n,q)$ に属するならば，

$$x=\omega^e\,(0\leqq e<q-1), \qquad x^n=1$$

と表せるので，

$$ne\equiv 0 \pmod{q-1}$$

が成り立つことになる．よって，e は f の倍数となり，X は $\langle A\rangle$ の元である．

3.2　射影線形群の置換表現

初めに，射影線形群が作用する射影空間の定義から述べよう．体 K 上の n 次元線形空間 $V=V(n,K)$ の 1 次元部分空間を**点**として，それら点の全体からなる集合を $n-1$ 次元**射影空間**といい，$PG(V)$ または $PG(n-1,K)$ で表す．ここで K が有限体 $GF(q)$ のとき，それを $PG(n-1,q)$ で表す．とくに，$PG(1,K)$ を K 上の**射影直線**，$PG(2,K)$ を K 上の**射影平面**という．また，V の 1 つの r 次元部分空間に含まれる 1 次元部分空間からなる集合を $PG(V)$ の $r-1$ 次元**部分空間**といい，$PG(V)$ の 1 次元部分空間を $PG(V)$ の**直線**，2 次元部分空間を $PG(V)$ の**平面**という．

本書では，以下 $V(n,K)$ を K 上の n 次行ベクトル全体からなる線形空間

として話を進めることにする．

$V(n,K)$ の $\mathbf{0}$(零ベクトル)でない元 v と $GL(n,K)$ の元 A に対し，$V(n,K)$ の $\mathbf{0}$ でない元 vA が定まる．そこで，$\langle v\rangle$ を v で生成された1次元部分空間とすると，$PGL(n,K)$ の元 $\bar{A}=A\cdot Z(GL(n,K))$ によって $PG(n-1,K)$ の元 $\langle v\rangle$ は，$PG(n-1,K)$ の1つの元 $\langle vA\rangle$ に移されることになる．明らかに，この対応によって $\bar{A}$ は $PG(n-1,K)$ 上の置換を引き起こすことが分かる．そして次の定理から，$PGL(n,K)$ や $PSL(n,K)$ は $PG(n-1,K)$ 上の置換群と見なせるのである(3.1節も参照)．

定　理 | 3.2.1

$GL(n,K)$ の元 A を $PG(n-1,K)$ 上に自然に作用させたとき，それが $PG(n-1,K)$ 上恒等的になるならば，A は $Z(GL(n,K))$ の元である．

証　明

明らかに $n\geqq 2$ としてよい．

V の $\mathbf{0}$ でない任意の2元 u,v をとると，仮定により

$$uA=\alpha u,\qquad vA=\beta v$$

とおくことができる $(\alpha,\beta\in K)$．ここで，$\alpha=\beta$ が成り立つことを示せばよい．

もし u と v が1次従属ならば，$u=\gamma v$ と表せるので$(\gamma\in K)$，

$$\alpha\gamma v=\alpha u=uA=\gamma(vA)=\gamma\beta v$$

から $\alpha=\beta$ がいえる．

一方，u と v が1次独立ならば，$(u+v)A=\delta(u+v)$ と表せるので $(\delta\in K)$，

$$\delta u+\delta v=(u+v)A=uA+vA=\alpha u+\beta v$$

から $\alpha=\delta=\beta$ がいえる．

定　理 | 3.2.2

$PSL(n,K)$ $(n\geqq 2)$ は $PG(n-1,K)$ 上の2重可移置換群である．

証　明

$\langle u_1\rangle, \langle u_2\rangle$ を $PG(n-1, K)$ の相異なる任意の2点とし，$\langle v_1\rangle, \langle v_2\rangle$ も $PG(n-1, K)$ の相異なる任意の2点とする．u_1, u_2 を含む $V(n, K)$ の基底 $\{u_1, u_2, \cdots, u_n\}$ と，v_1, v_2 を含む $V(n, K)$ の基底 $\{v_1, v_2, \cdots, v_n\}$ が存在し，

$$u_iA = v_i \qquad (i = 1, 2, \cdots, n)$$

となる $GL(n, K)$ の元 A が存在する．

いま $|A|(=\det A)=\alpha$ とおき，

$$u_1B = \frac{1}{\alpha}u_1, \qquad u_iB = u_i \qquad (i = 2, \cdots, n)$$

をみたす $GL(n, K)$ の元 B をとると，

$$(u_1, u_2, \cdots, u_n)BA = \left(\frac{1}{\alpha}v_1, v_2, \cdots, v_n\right)$$

$$|BA| = |B|\cdot|A| = \frac{1}{\alpha}\cdot\alpha = 1$$

となるので，$PSL(n, K)$ は $PG(n-1, K)$ 上2重可移に作用する．

定　理 | 3.2.3

$PGL(2, K)$ は $PG(1, K)$ 上3重可移置換群であり，$PGL(2, K)$ の3点の固定部分群 $PGL(2, K)_{\alpha\beta\gamma}$ は単位群になる．ただし，α, β, γ は $PG(1, K)$ の相異なる3点である．

証　明

最初に，定理3.2.2より $PGL(2, K)$ は $PG(1, K)$ 上2重可移であり，また

$$PG(1, K) = \{\langle(0, 1)\rangle, \langle(1, 0)\rangle\} \cup \{\langle(1, a)\rangle \mid a \in K^*\}$$

が成り立つ．そこで，

$$\alpha = \langle(0, 1)\rangle, \qquad \beta = \langle(1, 0)\rangle$$

とおいて，$PGL(2, K)_{\alpha\beta}$ の $\{\langle(1, a)\rangle \mid a \in K^*\}$ 上の作用を考えよう．

いま，$GL(2, K)$ の元 A に対し

$$(0, 1)A = (0, b), \qquad (1, 0)A = (c, 0) \qquad (b, c \in K^*)$$

とすると，

$$A=\begin{pmatrix} c & 0 \\ 0 & b \end{pmatrix}$$

が成り立つ．よって，

$$PGL(2,K)_{\alpha\beta}=\left\{\overline{\begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix}}\ \middle|\ d\in K^*\right\}$$

となるが，$\left\{\overline{\begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix}}\ \middle|\ d\in K^*\right\}$ は $\{\langle(1,a)\rangle \mid a\in K^*\}$ 上可移に作用する．したがって，定理 2.2.1 より $PGL(2,K)$ は $PG(1,K)$ 上の 3 重可移置換群である．さらに，$\gamma=\langle(1,1)\rangle$ とおけば，明らかに

$$PGL(2,K)_{\alpha\beta\gamma}=\left\{\overline{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}}\right\}$$

である．$PGL(2,K)$の 3 重可移性から，上式の α，β，γ は任意の相異なる 3 点としてよい．

3.3 可移拡大と可移置換群のランク

G を集合 Ω 上の置換群とし，$\bar{G}$ を $\bar{\Omega}=\Omega\cup\{\infty\}$ 上の置換群とする ($\infty\notin\Omega$)．もし $\bar{G}$ が $\bar{\Omega}$ 上可移で，∞ の固定部分群 $\bar{G}_\infty$ が G と一致するならば，$\bar{G}$ を G の**可移拡大**といい，G は**可移拡大可能**であるという．

3.4 節では，21 個の点からなる $PG(2,4)$ 上の 2 重可移置換群 $PSL(3,4)$ は可移拡大が 3 回可能であることを示す．そして，それらは順に 22 文字上の**マシュー群** M_{22}，23 文字上の**マシュー群** M_{23}，24 文字上の**マシュー群** M_{24} とよばれるものである．さらに，$GF(9)$ 上の位数が 72 の 2 重可移置換群 G を構成し，それも可移拡大が 3 回可能であることを示す．そして，それを 2 回可移拡大したものと 3 回可移拡大したものをそれぞれ 11 文字上の**マシュー群** M_{11}，12 文字上の**マシュー群** M_{12} という．なお，G を可移拡大した 10 文字上の 3 重可移置換群を本書では便宜上 M_{10} と書くことにするが，一般にはその記法は用いられない．

可移拡大に関する次の定理が，マシュー群を構成するときに本質的な役割を果たすことになる．

定 理 | 3.3.1

G を Ω 上の t 重可移置換群とする ($t \geqq 2$). h を $(\infty)h \in \Omega$ となる $\overline{\Omega} = \Omega \cup \{\infty\}$ 上の置換とし，以下の 3 条件をみたす $g \in G$ と $\alpha \in \Omega$ があるとする.

(1) $g \notin G_\alpha$

(2) $h^2 = (gh)^3 = 1$

(3) $hG_\alpha h = G_\alpha$

このとき，G を $(S^{\overline{\Omega}})_\infty$ の部分群とみなし，

$$\overline{G} = G \cup GhG$$

とおけば，$\overline{G}$ は $\overline{\Omega}$ 上の置換群で，G の可移拡大となる.

上の定理を証明するために，いくつかの準備を行おう.

一般に群 G と G の元 g と部分群 H, K に対し，G の部分集合 HgK を G における g を含む (H, K) の**両側剰余類**という．相異なる (H, K) の両側剰余類全体を $\{Hg_iK\}_{i \in I}$ で表すとき，

$$G = \sum_{i \in I} Hg_iK \qquad (\text{直和})$$

が成り立ち，上式を G の (H, K) による**両側分解**という.

次に G を Ω 上の可移置換群とし ($|\Omega| \geqq 2$)，α を Ω の元とするとき，G_α の Ω における軌道の個数を G の**ランク**といい，それを r で表すことが普通である．明らかに，$r = 2$ は G が Ω 上 2 重可移であるための必要十分条件である.

定 理 | 3.3.2

G を Ω 上の可移置換群 ($|\Omega| \geqq 2$)，α を Ω の元とする．G の (G_α, G_α) による両側分解の個数は G のランクと一致する．とくに G が Ω 上 2 重可移ならば，$G - G_\alpha$ の任意の元 g に対し，

$$G = G_\alpha \cup G_\alpha g G_\alpha \qquad (\text{直和})$$

が成り立つ.

証　明

Gの元x, yに対して，

$$G_\alpha x G_\alpha = G_\alpha y G_\alpha \Longleftrightarrow x \in G_\alpha y G_\alpha$$
$$\Longleftrightarrow (\alpha)x \in (\alpha)yG_\alpha$$
$$\Longleftrightarrow (\alpha)xG_\alpha = (\alpha)yG_\alpha$$

が成り立つ．これは，Gの(G_α, G_α)による両側分解の個数はGのランクと一致することを意味する．後半は明らかである．

定理 3.3.1 の証明

もし$\overline{G}$が$\overline{\Omega}$上の置換群であることを示すことができれば，$(\infty)h \in \Omega$と$\overline{G}_\infty = G$より，それがGの可移拡大になることは明らかである．

$$\overline{G} = G \cup GhG, \qquad h = h^{-1}$$

であるから，$\overline{G}$の各元の逆元は$\overline{G}$の元である．次に，$\overline{G}$が演算に関して閉じていることを示すために，

$$(GhG)(GhG) \subseteqq \overline{G},$$

すなわち

$$hGh \subseteqq \overline{G}$$

を示せばよい．仮定の(1)と定理 3.3.2 を使って，

$$G = G_\alpha \cup G_\alpha g G_\alpha \qquad (\text{直和})$$

と表せる．そして仮定の(2)と(3)を使って，

$$\begin{aligned} hGh &= h(G_\alpha \cup G_\alpha g G_\alpha)h \\ &= hG_\alpha h \cup hG_\alpha g G_\alpha h \\ &= G_\alpha \cup hG_\alpha (hg^{-1}hg^{-1}h) G_\alpha h \\ &= G_\alpha \cup (hG_\alpha h) g^{-1}hg^{-1} (hG_\alpha h) \\ &= G_\alpha \cup G_\alpha g^{-1}hg^{-1} G_\alpha \\ &\subseteqq G \cup GhG = \overline{G} \end{aligned}$$

を得る．

3.4　マシュー群の構成

E. Mathieu (1835-1890) はマシュー関数のように，数理物理方面で有名である．そしてマシュー群は，不変式の研究の過程で発見したものである．本節では，前節で紹介した方法にしたがってマシュー群を構成する．

最初に，定理 3.2.2 より $PSL(3,4)$ は $PG(2,4)$ 上の 2 重可移置換群であるが，

$$PG(2,4) \text{ の点の個数} = \frac{4^3-1}{4-1} = 21$$

に注意する．また，乗法群 $GF(4)^*$ は巡回群なので(定理 1.8.8 参照)，1 つの生成元 γ がある．

$PG(2,4)$ からそれ自身への次のような写像 $\sigma_1, \sigma_2, \sigma_3$ を考える．

$$\langle(x,y,z)\rangle\sigma_1 = \langle(x^2+yz, y^2, z^2)\rangle$$
$$\langle(x,y,z)\rangle\sigma_2 = \langle(x^2, y^2, z^2\gamma)\rangle$$
$$\langle(x,y,z)\rangle\sigma_3 = \langle(x^2, y^2, z^2)\rangle$$

ここで，

$$0^2=0, \quad 1^2=1, \quad \gamma^2=\gamma^2, \quad (\gamma^2)^2=\gamma,$$
$$(x^2+yz)^2+y^2z^2 = x^4+y^2z^2+y^2z^2 = x,$$
$$(y^2)^2=y, \quad (z^2)^2=z$$

なので，σ_1 は $PG(2,4)$ 上の位数 2 の置換である．同様にして，σ_2 と σ_3 が $PG(2,4)$ 上の位数 2 の置換であることも分かる．

いま，$\langle(1,0,0)\rangle\sigma_1 = \langle(1,0,0)\rangle$ であることに留意して，

$$\Omega = PG(2,4), \quad G = PSL(3,4), \quad \bar{\Omega} = \Omega \cup \{\infty\},$$
$$\alpha = \langle(1,0,0)\rangle,$$
$$g = \overline{\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}}, \qquad h_1 = \begin{cases} \Omega - \{\langle(1,0,0)\rangle\} \text{ 上では } \sigma_1 \\ \{\langle(1,0,0)\rangle, \infty\} \text{ 上では} \\ \quad \text{互換 } (\langle(1,0,0)\rangle, \infty) \end{cases}$$

とおくと，定理 3.3.1 の 3 条件をみたすことが以下のようにして分かる．

$$\langle(1,0,0)\rangle g = \langle(0,1,0)\rangle, \qquad h_1^2 = 1$$

は明らかである．次に，$(gh_1)^3 = 1$ であることを示そう．$g \in (S^{\bar{\Omega}})_\infty$ に留意し

て,

$$\langle(1,0,0)\rangle(gh_1)^3 = \langle(0,1,0)\rangle(gh_1)^2$$
$$= (\infty)\,gh_1$$
$$= \langle(1,0,0)\rangle$$
$$\langle(0,1,0)\rangle(gh_1)^3 = (\infty)\,(gh_1)^2$$
$$= \langle(1,0,0)\rangle(gh_1)$$
$$= \langle(0,1,0)\rangle$$

そして $\langle(x,y,z)\rangle \neq \langle(1,0,0)\rangle$, $\langle(0,1,0)\rangle$ のとき,

$$\langle(x,y,z)\rangle(gh_1)^3$$
$$= \langle(y^2+xz, x^2, z^2)\rangle(gh_1)^2$$
$$= \langle(x+(y^2+xz)z^2, y+x^2z^2, z)\rangle(gh_1)$$
$$= \langle(y^2+xz+xz+(y^2+xz)z^3, x^2+(y+x^2z^2)z, z^2)\rangle$$
$$= \langle(xz+y^2(z^3+1), yz+x^2(z^3+1), z^2)\rangle.$$

ここで, もし $z \neq 0$ ならば $z^3=1$ なので,

$$\langle(x,y,z)\rangle(gh_1)^3 = \langle(xz, yz, z^2)\rangle = \langle(x,y,z)\rangle$$

が成り立つ. また, もし $z=0$ ならば $xy \neq 0$ の場合を考えているので, すなわち $x, y \in \{1, \gamma, \gamma^2\}$ なので,

$$\langle(x,y,z)\rangle(gh_1)^3 = \langle(y^2, x^2, 0)\rangle = \langle(x,y,0)\rangle$$

となることが分かる.

以上から, 定理 3.3.1 の(1), (2)についてはみたしている. そして(3)についてもみたしていることを示すためには, $h_1G_\alpha h_1 \subseteqq G_\alpha$ を示せばよい. そこで, A を $\overline{A} \in G_\alpha$ となる $SL(3,4)$ の元とする.

$$\langle(1,0,0)\rangle\overline{A} = \langle(1,0,0)\rangle$$

であるから,

$$A = \begin{pmatrix} 1 & 0 & 0 \\ a & b & c \\ d & e & f \end{pmatrix}$$

としてよい. また, $A \in SL(3,4)$ より,

$$bf - ce = 1$$

である．さて，

$$\langle(1,0,0)\rangle h_1\bar{A}h_1=\langle(1,0,0)\rangle$$

は明らかであるが，それは必ずしも $h_1\bar{A}h_1\in G_\alpha$ を意味していないことに注意する．ここで $\langle(x,y,z)\rangle h_1\bar{A}h_1$ を計算すると，

$$\begin{aligned}&\langle(x,y,z)\rangle h_1\bar{A}h_1\\&\quad=\langle(x^4+y^2z^2+a^2y^4+d^2z^4+bcy^4+bfy^2z^2+cey^2z^2+efz^4,\\&\qquad\quad b^2y^4+e^2z^4,\ c^2y^4+f^2z^4)\rangle\end{aligned}$$

となる．そして，

$$x^4=x,\quad y^4=y,\quad z^4=z,\quad -1=1$$

$$bfy^2z^2+cey^2z^2+y^2z^2=(bf-ce+1)\,y^2z^2=0$$

であるので，

$$\langle(x,y,z)\rangle h_1\bar{A}h_1=\langle(x,y,z)\rangle\overline{\begin{pmatrix}1&0&0\\a^2+bc&b^2&c^2\\d^2+ef&e^2&f^2\end{pmatrix}}$$

を得る．ここで，

$$\begin{vmatrix}1&0&0\\a^2+bc&b^2&c^2\\d^2+ef&e^2&f^2\end{vmatrix}=b^2f^2-c^2e^2=(bf-ce)^2=1$$

なので，

$$\overline{\begin{pmatrix}1&0&0\\a^2+bc&b^2&c^2\\d^2+ef&e^2&f^2\end{pmatrix}}\in PSL(3,4).$$

以上から定理 3.3.1 により，$PG(2,4)$ 上の 2 重可移置換群 $PSL(3,4)$ は可移拡大できることになり，それが 22 文字上の**マシュー群** M_{22} である．ちなみに，

$$|M_{22}|=22\cdot|PSL(3,4)|=22\cdot|SL(3,4)|/3=22\cdot21\cdot20\cdot48.$$

次に，

$$\Omega=PG(2,4)\cup\{\infty\},\qquad G=M_{22},\qquad \bar{\Omega}=\Omega\cup\{\infty'\},\qquad \alpha=\infty,$$

$$g=h_1,\qquad h_2=\begin{cases}\Omega-\{\infty\}\ \text{上では}\ \sigma_2\\\{\infty,\infty'\}\ \text{上では互換}\ (\infty,\infty')\end{cases}$$

とおいて上と同様な議論を展開すれば，定理 3.3.1 により M_{22} も可移拡大できることがやさしく確かめられる．それが 23 文字上の**マシュー群** M_{23} で，

$$|M_{23}| = 23 \cdot |M_{22}| = 23 \cdot 22 \cdot 21 \cdot 20 \cdot 48$$

である．

さらに，

$$\Omega = PG(2,4) \cup \{\infty, \infty'\}, \qquad G = M_{23},$$

$$\bar{\Omega} = \Omega \cup \{\infty''\}, \qquad \alpha = \infty',$$

$$g = h_2, \qquad h_3 = \begin{cases} \Omega - \{\infty, \infty'\} \text{ 上では } \sigma_3 \\ \{\infty', \infty''\} \text{ 上では互換 } (\infty', \infty'') \\ \infty \text{ は固定} \end{cases}$$

とおいて上と同様な議論を展開すれば，定理 3.3.1 により M_{23} も可移拡大できることがやさしく確かめられる．それが 24 文字上の**マシュー群** M_{24} で，

$$|M_{24}| = 24 \cdot |M_{23}| = 24 \cdot 23 \cdot 22 \cdot 21 \cdot 20 \cdot 48$$

である．

以下，11 文字上のマシュー群 M_{11}，12 文字上のマシュー群 M_{12} を構成するが，$K = GF(9)$ 上の 2 重可移置換群の構成から始める．

定理 1.8.8 より

$$K = \{0, 1, \gamma, \gamma^2, \cdots, \gamma^7\}$$

となる K^* の元 γ が存在し，K の標数は 3 で $\gamma^4 = -1$ であるから，

$$(\gamma^2 + \gamma - 1)(\gamma^2 - \gamma - 1) = \gamma^4 + 1 = 0$$

を得る．したがって，必要ならば γ の代わりに $-\gamma$ をとることにすれば，γ は

$$\gamma^2 + \gamma - 1 = 0$$

をみたすとしてよい．

いま $K^* \ni \alpha$ に対して，K の自己同型写像 $\theta(\alpha)$ を

$$\theta(\alpha) = \begin{cases} 1_K & (\alpha \in \{1, \gamma^2, \gamma^4, \gamma^6\}) \\ \langle x \longmapsto x^3 \rangle & (\alpha \in \{\gamma, \gamma^3, \gamma^5, \gamma^7\}) \end{cases}$$

とおく．ここで，1_K は K の恒等写像で，$\langle x \mapsto x^3 \rangle$ は K のすべての元をそれぞれ 3 乗する K の自己同型写像である．なお，$\langle x \mapsto x^3 \rangle$ が K の自己同型写像に

なることはやさしく確かめられる．また，$\theta^2 = 1_K$ に注意する．そして，$K \ni \alpha$ $(\neq 0)$，β に対して K 上の置換

$$\sigma(\alpha, \beta) : x \longmapsto \alpha \cdot x^{\theta(\alpha)} + \beta \qquad (x \in K)$$

を定め，そのような置換全体からなる集合

$$G = \{\sigma(\alpha, \beta) \mid K \ni \alpha\,(\neq 0), \beta\}$$

を考えると，G は K 上の置換群になる．

実際，K の任意の元 x に対して，

$$\begin{aligned}(x)\sigma(\alpha_1, \beta_1)\sigma(\alpha_2, \beta_2) &= (\alpha_1 \cdot x^{\theta(\alpha_1)} + \beta_1)\sigma(\alpha_2, \beta_2) \\ &= \alpha_2(\alpha_1 \cdot x^{\theta(\alpha_1)} + \beta_1)^{\theta(\alpha_2)} + \beta_2 \\ &= \alpha_2 \cdot \alpha_1{}^{\theta(\alpha_2)}(x^{\theta(\alpha_1)})^{\theta(\alpha_2)} + \alpha_2 \cdot \beta_1^{\theta(\alpha_2)} + \beta_2 \\ &= \alpha_2 \cdot \alpha_1{}^{\theta(\alpha_2)}(x)^{\theta(\alpha_1)\theta(\alpha_2)} + \alpha_2 \cdot \beta_1{}^{\theta(\alpha_2)} + \beta_2.\end{aligned}$$

ここで，

$$\theta(\alpha_1)\theta(\alpha_2) = \theta(\alpha_2 \cdot \alpha_1^{\theta(\alpha_2)})$$

が成り立つので，

$$\sigma(\alpha_1, \beta_1)\sigma(\alpha_2, \beta_2) = \sigma(\alpha_2 \cdot \alpha_1{}^{\theta(\alpha_2)}, \alpha_2 \cdot \beta_1^{\theta(\alpha_2)} + \beta_2)$$

を得る．よって，G は写像の合成に関して閉じている．また，

$$\sigma(\alpha, \beta)^{-1} = \sigma((\alpha^{-1})^{\theta(\alpha)}, (-\alpha^{-1}\beta)^{\theta(\alpha)})$$

が成り立ち，$\sigma(1, 0)$ は G の単位元である．

以上から G は K 上の置換群になるが，さらに G は K 上 2 重可移に作用する．なぜならば，K の異なる任意の 2 元 α, β に対して，$\sigma(\beta - \alpha, \alpha)$ は 0 を α に移し，1 を β に移すからである．そして，次のことが分かる：

$$G_0 = \{\sigma(\alpha, 0) \mid K \ni \alpha \neq 0\}, \qquad |G_0| = 8,$$

$$G_{0,1} = \{\sigma(1, 0)\}, \qquad |G_{0,1}| = 1,$$

$$|G| = 9 \cdot 8 = 72.$$

以下，定理 3.3.1 をくり返し用いて G を可移拡大していく．いま，

$$\Omega = K, \qquad \bar{\Omega} = \Omega \cup \{\infty\}, \qquad \alpha = 0,$$

$$g = \sigma(-1, 1) = \langle x \longmapsto 1 - x \rangle,$$

$$h_1 = \begin{cases} K^* \text{ 上では } \langle x \longmapsto x^{-1} \rangle \\ \{0, \infty\} \text{ 上では互換 } (0, \infty) \end{cases}$$

とおけば，$g \notin G_\alpha$，$h_1^2 = 1$ であることは明らか．また，$0, 1, \infty, K - \{0, 1\}$ の 4 種類の任意の元に作用させて考えれば，$(gh_1)^3 = 1$ が成り立つことが分かる．よって，定理 3. 3. 1 の条件(1)，(2)についてはみたしている．

また，G_0 の任意の元は $\sigma(\alpha, 0)$ $(\alpha \in K^*)$ で表され，

$$h_1 \cdot \sigma(\alpha, 0) \cdot h_1 = \sigma(\alpha^{-1}, 0)$$

となるので，$h_1 G_0 h_1 \subseteqq G_0$ が成り立つ．よって，(3)についてもみたしている．したがって，K 上の 2 重可移置換群 G は可移拡大できることになり，それを本書では M_{10} と書くことにする．ちなみに，

$$|M_{10}| = 10 \cdot |G| = 10 \cdot 9 \cdot 8.$$

次に，

$$\Omega = K \cup \{\infty\}, \qquad G = M_{10}, \qquad \bar{\Omega} = \Omega \cup \{\infty'\}, \qquad \alpha = \infty,$$

$$g = h_1, \qquad h_2 = \begin{cases} K \text{ 上では } \langle x \longmapsto \gamma^2 x + \gamma x^3 \rangle \\ \{\infty, \infty'\} \text{ 上では互換 } (\infty, \infty') \end{cases}$$

とおいて上と同様な議論を展開すれば，途中の計算はやや長くなるものの，定理 3. 3. 1 により M_{10} も可移拡大できることがやさしく確かめられる．それが 11 文字上の**マシュー群** M_{11} で，

$$|M_{11}| = 11 \cdot |M_{10}| = 11 \cdot 10 \cdot 9 \cdot 8$$

である．

さらに，

$$\Omega = K \cup \{\infty, \infty'\}, \qquad G = M_{11}, \qquad \bar{\Omega} = \Omega \cup \{\infty''\}, \qquad \alpha = \infty',$$

$$g = h_2, \qquad h_3 = \begin{cases} K \text{ 上では } \langle x \longmapsto x^3 \rangle \\ \{\infty', \infty''\} \text{ 上では互換 } (\infty', \infty'') \\ \infty \text{ は固定} \end{cases}$$

とおいて上と同様な議論を展開すれば，定理 3. 3. 1 により M_{11} も可移拡大できることがやさしく確かめられる．それが 12 文字上の**マシュー群** M_{12} で，

$$|M_{12}| = 12 \cdot |M_{11}| = 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8$$

である．

なお，5 つのマシュー群 $M_{22}, M_{23}, M_{24}, M_{11}, M_{12}$ は単純群であることが知られている([和；9] 参照)．

3.5　多重可移置換群の単純性

有限多重可移置換群であるマシュー群 $M_{22}, M_{23}, M_{24}, M_{11}, M_{12}$ や交代群 A_n ($n \geqq 5$) は単純群になるが，本節ではそれらの説明で本質的に重要な定理 3.5.3 と 3.5.4 を紹介し，それらの説明の概略を述べることにする．

定　理｜3.5.1

G を Ω 上の原始置換群とし，N を単位群と異なる G の正規部分群とすると，N は Ω 上可移である．

証　明

$N \neq 1$ であるから，$|(\alpha)N| > 1$ をみたす Ω の元 α がある．そして，G の元 g に対し

$$((\alpha)N)g \cap (\alpha)N \neq \emptyset$$

とすると，$((\alpha)N)g = ((\alpha)g)N$ であるから，$(\alpha)N$ と $((\alpha)g)N$ は共通の元をもつ N の軌道である．よって，

$$((\alpha)N)g = ((\alpha)g)N = (\alpha)N$$

となり，$(\alpha)N$ は G のブロックである．

したがって，G は Ω 上の原始置換群なので，$(\alpha)N = \Omega$ でなければならない．

定　理｜3.5.2

$G \neq 1$ が Ω 上の原始置換群ならば，G_α は G の極大部分群である ($\alpha \in \Omega$)．

証　明

もし

$$G_\alpha < H < G$$

となる G の部分群 H があるならば，明らかに $(\alpha)H \supsetneqq \{\alpha\}$ であり，$(\alpha)H$ は G のブロックになる．実際，G の元 g に対し

$$((\alpha)H)g \cap (\alpha)H \neq \emptyset$$

とすると，H のある元 h_1, h_2 に対し

$$(\alpha)h_1g=(\alpha)h_2$$

となる．したがって，$h_1gh_2^{-1}\in G_\alpha$，すなわち

$$g\in h_1^{-1}G_\alpha h_2\subseteqq H$$

である．よって，$((\alpha)H)g=(\alpha)H$ でなければならない．

また上の議論は，$g\in G-H$ ならば

$$((\alpha)H)g\cap(\alpha)H=\emptyset$$

であることも意味している．

以上から，$(\alpha)H$ は自明でない G のブロックとなり，これは仮定に反して矛盾である．

定　理 | 3. 5. 3

G を Ω 上の原始置換群とし，G_α は単純群とする ($\alpha\in\Omega$)．このとき，もし G が単純群でないならば，G は Ω 上正則な正規部分群 N をもつ．

証　明

仮定より G は $1<N<G$ をみたす正規部分群 N をもち，定理3.5.1により N は Ω 上可移である．また，すべての $\alpha\in\Omega$ に対し

$$N\cap G_\alpha\trianglelefteqq G_\alpha$$

が成り立つ．ここで G_α は単純群であるから，

(i)　すべての $\alpha\in\Omega$ に対して $N\cap G_\alpha=1$

または

(ii)　すべての $\alpha\in\Omega$ に対して $N\cap G_\alpha=G_\alpha$

が成り立つ．(ii)の場合は $G_\alpha\subseteqq N$ となるが，N は Ω 上可移なので，$G_\alpha\subsetneqq N$ である．これは，定理3.5.2に反して矛盾である．よって(i)の場合が成り立ち，N は Ω 上正則となる．

さて，ここで G は Ω 上の可移置換群で，Ω 上正則な正規部分群 N をもつとしよう．Ω の1つの元 α を固定すると，$\Omega-\{\alpha\}$ の任意の元 β に対し，$(\alpha)n_\beta$

$=\beta$ となる $N-\{1\}$ の元 n_β が一意的に存在する．この対応によって，$\Omega-\{\alpha\}$ から $N-\{1\}$ への全単射 φ が定義できる．G_α は $\Omega-\{\alpha\}$ 上の置換群と見なせるが，この φ を通して置換群として同型な $N-\{1\}$ 上の置換群 G_α が以下のようにして定められる．

$\Omega-\{\alpha\}$ の元 β, γ と G_α の元 g に対し，

$$
\begin{aligned}
(\beta)g=\gamma &\Longleftrightarrow (\alpha)n_\beta g = (\alpha)n_\gamma \\
&\Longleftrightarrow (\alpha)g^{-1}n_\beta g = (\alpha)n_\gamma \\
&\Longleftrightarrow g^{-1}n_\beta g = n_\gamma
\end{aligned}
$$

であるから，G_α の任意の元 g の $N-\{1\}$ 上の作用は，$N-\{1\}$ のすべての元 n を $n^g=g^{-1}ng$ に移せばよい．

もし，G_α が $\Omega-\{\alpha\}$ 上可移に作用するならば，G_α は $N-\{1\}$ 上可移に作用することになる．これは，$N-\{1\}$ のすべての元の位数はある素数に等しいことなどがすぐ導かれるように，極めて強い性質なのである．

上で述べたようにして考えると，簡単な議論を重ねて次の結果を得る([洋；16] 参照)．

定　理 | 3.5.4

G を有限集合 Ω 上の t 重可移置換群とし，N を Ω 上正則な正規部分群とすると，$t \leqq 4$ であり，以下が成り立つ．

(1)　$t=2$ のとき，N は位数 p^m (p は素数)の基本可換群である．

(2)　$t=3$ のとき，N は位数 2^m の基本可換群であるか位数 3 の巡回群である．

(3)　$t=4$ のとき，G は 4 次対称群である．

5 つのマシュー群 $M_{22}, M_{23}, M_{24}, M_{11}, M_{12}$ および交代群 A_n ($n \geqq 5$) が単純群であることの証明は，以下のようにしてできる．

最初に，$A_5, PSL(3,4), M_{11}$ の単純性を示す．次にそれらの可移拡大である A_6, M_{22}, M_{12} が単純群でないならば，定理 3.5.3 を用いて，可移拡大した置換群 G は正則な正規部分群 N をもつ．ところが，定理 3.5.4 によってその N は

具体的な形として表され，それによって矛盾が導かれる．他の交代群やマシュー群の単純性についても，順次同様にして示す．

3.6 マシュー群のデザイン論的性質

本節では，4章で扱う内容の準備として，マシュー群のデザイン論的性質について述べる．

最初に，マシュー群 M_{23} の4点の固定部分群について述べよう．

$$|PSL(3,4)| = 21 \cdot 20 \cdot 48, \qquad |PG(2,4)| = 21$$

であるから，$PSL(3,4)$ の2点の固定部分群の位数は48である．M_{23} の4点の固定部分群は，$PSL(3,4)$ の $PG(2,4)$ 上の2点 $\langle(1,0,0)\rangle$，$\langle(0,1,0)\rangle$ の固定部分群と置換群として同型になるが，この2点の固定部分群は

$$\left\{ \overline{\begin{pmatrix} 1 & 0 & 0 \\ 0 & c & 0 \\ a & b & c^{-1} \end{pmatrix}} \middle| \, c \in GF(4)^*, \ \ a, b \in GF(4) \right\}$$

であることがやさしく分かる．さらにこの群は，位数3の部分群

$$V = \left\{ \overline{\begin{pmatrix} 1 & 0 & 0 \\ 0 & c & 0 \\ 0 & 0 & c^{-1} \end{pmatrix}} \middle| \, c \in GF(4)^* \right\}$$

と，位数16の正規部分群

$$P = \left\{ \overline{\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ a & b & 1 \end{pmatrix}} \middle| \, a, b \in GF(4) \right\}$$

の半直積となることが分かる．ここで，P は基本可換群であることも直接確かめられる．

さて，P は $\langle(x,y,0)\rangle$ という形をした $PG(2,4)$ の5点をそれぞれ点として固定する．一方，P は $PG(2,4)$ のそれ以外の点の集合上では正則に作用している(定理2.1.3参照)．P は M_{23} の4点の固定部分群のシロー2-部分群と見なすことができ，$G = M_{23}$ とおくと，定理2.2.4と2.2.7により $N_G(P)^{I(P)}$ は A_7 または S_7 になることがやさしく分かる．さらに，P は G の4点の固定部分群のシロー2-部分群であることに注目すれば，

$$N_G(P)^{I(P)} = A_7$$

に限ることが分かる．ここで，$I(P)$ の任意の異なる 4 点 $\alpha, \beta, \gamma, \delta$ に対しても，P は $G_{\alpha\beta\gamma\delta}$ の唯一のシロー 2-部分群であることに注意する．なお，$G = M_{22}$ として，P を G の 3 点の固定部分群のシロー 2-部分群と見なせば $N_G(P)^{I(P)} = A_6$ であり，$I(P)$ の任意の異なる 3 点 α, β, γ に対し，P は $G_{\alpha\beta\gamma}$ の唯一のシロー 2-部分群である．また，$G = M_{24}$ として，P を G の 5 点の固定部分群のシロー 2-部分群と見なせば $N_G(P)^{I(P)} = A_8$ であり，$I(P)$ の任意の異なる 5 点 $\alpha, \beta, \gamma, \delta, \varepsilon$ に対し，P は $G_{\alpha\beta\gamma\delta\varepsilon}$ の唯一のシロー 2-部分群である．

次に，Ω 上の置換群 G をマシュー群 M_{11} と置換群として同型なものとして，$|\Delta| = 4$ となる Ω の部分集合 Δ に対し，G における Δ の集合としての固定部分群 $G_{(\Delta)}$ の軌道を考えよう．

明らかに，

$$|G_\Delta| = 1, \qquad (G_{(\Delta)})^\Delta = S_4$$

が成り立つ．よって $|G_{(\Delta)}| = 24$ となるが，これは，Δ を集合として固定している G の元は，Δ 上の作用だけから一意的に定まることを意味している．そして，$G_{(\Delta)}$ の $\Omega - \Delta$ 上の軌道は，1 個の元からなる集合と 6 個の元からなる集合の 2 つとなることが以下のようにして分かる．

3.4 節で M_{10} を構成していくときに用いた K 上の 2 重可移置換群 G において，

$$G_0 = \{\sigma(\alpha, 0) \mid K \ni \alpha \neq 0\}, \qquad |G_0| = 8$$

であった．G_0 の単位元と異なる各元の位数を具体的に調べると，位数 2 の元が 1 つだけあって，他の元はすべて位数 4 である．G_0 は位数 8 の**四元数群**と一般によばれるものであるが，ここでは，G_0 の中心に属するその位数 2 の元に注目する(定理 1.7.1 参照)．

いま，

$$\Omega = \{1, 2, 3, \cdots, 11\}, \qquad \Delta = \{1, 2, 3, 4\}$$

とおいて，a を次の形をした G の位数 2 の元としてよい(G は 3.4 節のものでなく本節のもの)．

$$a = (1)(2)(3)(4\quad 5)(6\quad 7)(8\quad 9)(10\quad 11)$$

G は Ω 上 4 重可移であるから，次の形をした元 b をもつ．

$$b = (1\quad 2)(3)(4)\cdots$$

ここで，$b^{-1}G_{123}b = G_{123}$ であるから，G_{123} の唯一の位数 2 の元 a に対して，

$$b^{-1}ab = a$$

でなくてはならない．それゆえ，

$$b = (1\quad 2)(3)(4)(5)\cdots$$

となるが，さらに

$$b^2 = (1)(2)(3)(4)(5)\cdots \in G_{12345}$$

となるので，b は G_{345} の位数 2 の元になる．

同様にして，G は a と可換な次の形をした位数 2 の元 c をもつことが分かる．

$$c = (1\quad 3)(2)(4)(5)\cdots$$

したがって $\langle b, c\rangle$ を考えれば，$(G_{4,5})_{(\{1,2,3\})}$ は $\{1, 2, 3\}$ 上に 3 次対称群として作用することがいえる．これは a に対していえることに留意すれば，b に対して $(G_{1,2})_{(\{3,4,5\})}$ は $\{3, 4, 5\}$ 上に 3 次対称群として作用することがいえる．よって，$G_{(\{1,2,3,4,5\})}$ は $\{1, 2, 3, 4, 5\}$ 上に 5 次対称群として作用する．

以上から，$G_{(\Delta)}$ の 24 個の元はすべて $\{5\}$ を固定することになり，$\{5\}$ は $G_{(\Delta)}$ の 1 つの軌道である．そして，$G_{(\Delta)}$ の $\Omega - \Delta$ 上の $\{5\}$ 以外の任意の軌道 Γ をとると，$|\Gamma|$ は 6 以下の 24 の約数である．よって，$|\Gamma|$ は 1, 2, 3, 4, 6 のいずれかになるが，$G_{(\Delta)}$ の位数 2 の元

$$b = (1\quad 2)(3)(4)(5)\cdots$$

および位数 3 の元

$$bc = (1\quad 2\quad 3)(4)(5)\cdots$$

の Γ 上の作用を考えると，$|\Gamma| = 6$ 以外の場合は b または bc が Γ 上のある点を固定することになり，矛盾である．したがって，$|\Gamma| = 6$ でなければならない．

なお上の議論から，$\{1, 2, 3, 4, 5\}$ の任意の異なる 4 点からなる部分集合 $\{\alpha, \beta, \gamma, \delta\}$ に対して，$G_{(\{\alpha,\beta,\gamma,\delta\})}$ の 24 個のすべての元は $\{1, 2, 3, 4, 5\}$ を集合として固

定することに注意する．すなわち，$G_{(\{\alpha,\beta,\gamma,\delta\})}$ は1点からなる集合 $\{1,2,3,4,5\}-\{\alpha,\beta,\gamma,\delta\}$ を固定するのである．

以上から，M_{11} を可移拡大した M_{12} に関しては以下のことがいえる．Ω 上の置換群 G をマシュー群 M_{12} と置換群として同型なものとすれば，$|\varDelta|=5$ となる Ω の部分集合 $\varDelta$ に対し，$G_{(\varDelta)}$ の $\Omega-\varDelta$ 上の軌道も1個の元からなる集合 $\{\eta\}$ と6個の元からなる集合に分かれる．そして，$\varDelta\cup\{\eta\}$ の任意の異なる5点からなる部分集合 $\{\alpha,\beta,\gamma,\delta,\varepsilon\}$ に対して，$G_{(\{\alpha,\beta,\gamma,\delta,\varepsilon\})}$ の $\Omega-\{\alpha,\beta,\gamma,\delta,\varepsilon\}$ 上の1個の元からなる軌道は $\varDelta\cup\{\eta\}-\{\alpha,\beta,\gamma,\delta,\varepsilon\}$ である．

4章 群とデザイン

4.1 デザイン

デザインに関心をもつきっかけは統計学の実験計画であったり，符合理論であったり，置換群であったりするように，その応用は広い．そしてデザイン論は，グラフ理論と並んで組合せ論の中心的課題であったが，最近はグラフ理論の方が注目されているようである．なお，農業実験に起源をもつ「実験計画」は「design of experiments」の訳であり，それは1930年代にフィッシャーによって創始された．

v 個の元からなる有限集合 Ω と整数 k $(2 \leqq k \leqq v)$ に対し，

$$\Omega^{(k)} = \{X \mid |X| = k,\ X \subseteqq \Omega\}$$

とおく．明らかに $|\Omega^{(k)}| = \binom{v}{k}$ である．いま，自然数 λ と t $(\leqq k)$ に対し次の条件をみたす $\Omega^{(k)}$ の部分集合 $\boldsymbol{B}$ があるとき，Ω と $\boldsymbol{B}$ の組 $(\Omega, \boldsymbol{B})$ を t-(v, k, λ) **デザイン**，あるいは単に t-**デザイン**という：Ω の相異なる任意の t 個の元 $\alpha_1, \alpha_2, \cdots, \alpha_t$ に対し，それらを含む $\boldsymbol{B}$ の元はちょうど λ 個ある．

Ω の元を点，$\boldsymbol{B}$ の元をブロックという．また，Ω を点集合，$\boldsymbol{B}$ をブロック集合という．そして，$\boldsymbol{B} = \Omega^{(k)}$ であるデザインを自明なデザインという．明らかに，$t = k$ あるいは $k = v$ ならば自明である．

2つの t-(v, k, λ) デザイン $D_1 = (\Omega_1, \boldsymbol{B}_1)$，$D_2 = (\Omega_2, \boldsymbol{B}_2)$ に対し，Ω_1 から Ω_2 への全単射 φ があって，

$$B \in \boldsymbol{B}_1 \Longleftrightarrow (B)\varphi \in \boldsymbol{B}_2$$

が成り立つとき，φ を D_1 から D_2 の上への**同型写像**であるといい，D_1 と D_2 は**同型**であるという．同じパラメーターでも同型でないデザインはたくさんあり，むしろ同型を除いて一意的に定まるパタメーターの方が珍しいと言える([洋；10] 参照)．そして，デザインの存在性が確認されているパラメーターに対して，同型を除いていくつのデザインが存在するかを決定することは意外と難し

いことである．

t-(v,k,λ) デザイン $D=(\Omega,\boldsymbol{B})$ に対し，D から D の上への同型写像全体からなる集合は写像の合成に関して群になるが，それを D の**自己同型群**といい $\mathrm{Aut}(D)$ で表す．また，$\mathrm{Aut}(D)$ の各元を D の**自己同型写像**という．明らかに $\mathrm{Aut}(D)$ は Ω 上の置換群である．

任意の自然数 t に対して自明でない t-デザインが存在することは分かっているが，その存在性が証明されたのは1980年代の後半である([論；33, 34] 参照)．

t-$(v,k,1)$ デザインをとくに**シュタイナーシステム** $S(t,k,v)$ という．3.6節よりシュタイナーシステム $S(4,5,11)$，$S(5,6,12)$，$S(3,6,22)$，$S(4,7,23)$，$S(5,8,24)$ の存在性がいえ，それらを順に**ウィットシステム** W_{11}，W_{12}，W_{22}，W_{23}，W_{24} とよぶ．ウィットシステムは同型を除いて一意的に定まること，および

$$\mathrm{Aut}(W_{11})=M_{11},\quad \mathrm{Aut}(W_{12})=M_{12},$$
$$\mathrm{Aut}(W_{22})=M_{22},\quad \mathrm{Aut}(W_{23})=M_{23},\quad \mathrm{Aut}(W_{24})=M_{24}$$

であることが知られている([洋；3] 参照)．

$t=5$ のシュタイナーシステム $S(5,k,v)$ は他にも発見されているが([論；9, 26] 参照)，$t\geqq 6$ のシュタイナーシステムは未だ発見されていない．当然，それについての研究はデザイン論にとって大変重要なことであり，符合理論にも大きな影響を及ぼすであろう．

次の定理は明らかである．

定理 | 4.1.1

$D=(\Omega,\boldsymbol{B})$ を t-(v,k,λ) デザインとする．Γ を $|\Gamma|=s\ (1\leqq s\leqq t-1)$ となる Ω の部分集合とする．このとき，

$$\boldsymbol{B}'=\{B-\Gamma\,|\,B\in\boldsymbol{B},\ \Gamma\subseteqq B\}$$

とおくと，$D'=(\Omega-\Gamma,\ \boldsymbol{B}')$ は $(t-s)$-$(v-s,\ k-s,\ \lambda)$ デザインである．

上の定理における D' を D からの**誘導デザイン**という．

定理 | 4.1.2

$D=(\Omega, \boldsymbol{B})$ を t-(v, k, λ) デザインとし，$0 \leqq s \leqq t-1$ に対し $\alpha_1, \alpha_2, \cdots, \alpha_s$ を Ω の相異なる s 個の元とする．このとき，それら s 個の元を含むブロックの個数 $n(\alpha_1, \alpha_2, \cdots, \alpha_s)$ は

$$\frac{(v-s)(v-s-1)\cdots(v-t+1)\lambda}{(k-s)(k-s-1)\cdots(k-t+1)}$$

に等しい．とくに，$n(\alpha_1, \alpha_2, \cdots, \alpha_s)$ は $\alpha_1, \alpha_2, \cdots, \alpha_s$ のとり方によらない数である．

証明

集合

$$\{(\{\beta_1, \beta_2, \cdots, \beta_{t-s}\}, B) \mid B \in \boldsymbol{B},\ \{\alpha_1, \cdots, \alpha_s, \beta_1, \cdots, \beta_{t-s}\} \subseteqq B\}$$

の要素の個数を，第 1 成分から求める場合と第 2 成分から求める場合の 2 通りで求めると，

$$\binom{v-s}{t-s}\lambda = n(\alpha_1, \alpha_2, \cdots, \alpha_s)\binom{k-s}{t-s}$$

を得る．よって，

$$n(\alpha_1, \alpha_2, \cdots, \alpha_s) = \frac{\binom{v-s}{t-s}\lambda}{\binom{k-s}{t-s}}$$

$$= \frac{(v-s)(v-s-1)\cdots(v-t+1)\lambda}{(k-s)(k-s-1)\cdots(k-t+1)}$$

が成り立つ．

上の定理から $n(\alpha_1, \alpha_2, \cdots, \alpha_s)$ は s のみによって定まるので，以後それを λ_s とおく．なお一般に，$\lambda_0 = |\boldsymbol{B}|$ を b で，λ_1 を r で表す．

$\lambda_0, \lambda_1, \cdots, \lambda_{t-1}$ はものの個数ゆえ整数であり，定理 4.1.2 は自明でない整数条件を意味している．

例 | 4.1.3

(ア) 2-(15,7,3)デザインは同型を除いてちょうど5個あることが知られているが([洋；4] 参照)，2-(15,7,λ)デザイン($\lambda = 1$ または 2)は存在しない．実際，もし存在するならば

$$r = \frac{14 \cdot \lambda}{6}$$

となるので，この場合 r は整数にならない．

(イ) シュタイナーシステム $S(6,7,13)$ は存在しない．なぜならば，もし存在すると

$$b = \frac{13 \cdot 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8}{7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2}$$

となって，b は整数にならないので矛盾である．なおこれにより，3.4節で構成したマシュー群 M_{12} は可移拡大できないことが分かる．同様にして，シュタイナーシステム $S(6,9,25)$ の非存在性と，M_{24} は可移拡大できないことが分かる．

2以上の整数 n に対し，2-$(n^2+n+1,\ n+1,\ 1)$ デザインを**位数** n **の射影平面**といい，2-$(n^2, n, 1)$ デザインを**位数** n **のアフィン平面**という．それらの存在性と1.9節で紹介した n 次ラテン方陣の完全直交系のそれは，次の定理から本質的に同じことである．

定　理 | 4.1.4

次の(1)，(2)，(3)は互いに同値である．

(1) 位数 n の射影平面が存在する．

(2) 位数 n のアフィン平面が存在する．

(3) n 次ラテン方陣の完全直交系が存在する．

上の定理を証明する前に，射影平面やアフィン平面の基本的な性質を述べよ

う．

定　理 | 4. 1. 5

$(\Omega, \boldsymbol{B})$ を位数 n の射影平面とすると，異なる任意のブロック B_1, B_2 に対して $|B_1 \cap B_2| = 1$ が成り立つ．

証　明

Ω の異なる任意の2点 α, β に対して，α と β を含むブロックはちょうど1つなので，

$$|B_1 \cap B_2| \leqq 1$$

でなくてはならない．もし $|B_1 \cap B_2| = 0$ となる2つのブロック B_1, B_2 があるとすると，B_1 の1つの固定した点 α と B_2 の各点 β に対し，α と β を含むブロック $B(\alpha, \beta) = B(\beta, \alpha)$ がそれぞれただ1つ定まるので，$n+1$ 個のブロック $B(\alpha, \beta_1), B(\alpha, \beta_2), \cdots, B(\alpha, \beta_{n+1})$ が定まる．ただし，$B_2 = \{\beta_1, \beta_2, \cdots, \beta_{n+1}\}$．このとき，

$$\begin{aligned}&|B_1 \cup B(\alpha, \beta_1) \cup B(\alpha, \beta_2) \cup \cdots \cup B(\alpha, \beta_{n+1})| \\ &\quad = (n+1) + n(n+1) > |\Omega|\end{aligned}$$

となって矛盾である．

定　理 | 4. 1. 6

$(\Omega, \boldsymbol{B})$ を位数 n のアフィン平面とする．任意の $B \in \boldsymbol{B}$ と $\alpha \in \Omega - B$ に対し，

$$B \cap B' = \emptyset, \qquad B' \ni \alpha$$

となるブロック B' がただ1つ存在する．さらに，B と互いに素(共通部分が空)なブロックはちょうど $n-1$ 個存在し，それらを $B_1, B_2, \cdots, B_{n-1}$ とすると，

$$\Omega = B \cup B_1 \cup B_2 \cup \cdots \cup B_{n-1} \qquad (\text{直和})$$

が成り立つ．

証　明

$$r=\frac{n^2-1}{n-1}=n+1$$

であるので，α を含むブロックは $n+1$ 個ある．いま，それらを $C_1, C_2, \cdots, C_{n+1}$ とし，$B=\{\beta_1, \beta_2, \cdots, \beta_n\}$ とおくと，各 $i\,(1\leqq i\leqq n)$ に対し α と β_i を含むブロック $B(\alpha, \beta_i)=B(\beta_i, \alpha)$ はただ1つ定まるので，それはある $C_j\,(1\leqq j\leqq n+1)$ になる．ところが，その対応によってちょうど1つの C_k が余ることになり，それが B' である．

次に，B' を B_1 とおき，$\Omega-(B\cup B_1)$ の任意の元 α' をとると，上と同じ議論によって，

$$B\cap B_2=\emptyset, \qquad B_2\ni\alpha'$$

となるブロック B_2 が存在する．ここで，$B_1\cap B_2=\emptyset$ である．なぜならば，もし $B_1\cap B_2\neq\emptyset$ とすると，$B_1\cap B_2$ の元 γ に対し，B_1 と B_2 は γ を含む B と互いに素なブロックとなる．しかしながら，これは前半の議論で α を γ に代えたものに矛盾する．

以下，上の議論を同様にくり返すことにより，後半の主張も証明される．

t-(v, k, λ) デザイン $D=(\Omega, \boldsymbol{B})$ において，一般に

$$\frac{b}{r}=\frac{v}{k}$$

であるが，もし $\boldsymbol{B}$ が次のように分解できるとき，D は**分解可能**であるという．ただし，$l=b/r$ である．

$$\boldsymbol{B}=\bigcup_{i=1}^{r}\{B_{i1}, B_{i2}, \cdots, B_{il}\},$$

$$\Omega=B_{i1}\cup B_{i2}\cup\cdots\cup B_{il} \qquad (\text{直和}) \quad (i=1,2,\cdots,r).$$

定理 4.1.6 は，位数 n のアフィン平面は分解可能 2-デザインであることを示している．分解可能デザインとなるものの研究は古くから行われており，次の例は有名である．

例 4.1.7 ……………………………… **カークマンの女子学生問題(1850 年)**

15 人の女子学生 $G_1, G_2, \cdots, G_{14}, G_\infty$ の 7 日間にわたる散歩を，次の条件をみたすように計画できるか．

(ア) 毎日 3 人ずつのグループを 5 つ作って，15 人全員が散歩する．

(イ) 15 人のうちのどの 2 人に対しても，その 2 人を含む散歩のグループは，7 日間を通してちょうど 1 つだけ存在する．

この問題の本質は，「分解可能な 2-(15, 3, 1) デザインは存在するか」というものである．結論は以下のようにして計画できる．

G_i, G_j, G_k 3 人の散歩のグループを $\{i, j, k\}$ と書くことにする．また，G_∞ 以外の任意の女子学生 G_h $(1 \leqq h \leqq 14)$ に関して，添字 h は 14 を法とする合同式で考えているものとする．各 i $(i = 1, 2, \cdots, 7)$ に対し，i 日目の散歩のグループを次の 5 つとすれば，それは 1 つの解になることが具体的にチェックすることによって確かめられる．

$$S_i = \{\infty,\ 1+2(i-1),\ 2+2(i-1)\},$$
$$T_i = \{3+2(i-1),\ 5+2(i-1),\ 9+2(i-1)\},$$
$$U_i = \{4+2(i-1),\ 11+2(i-1),\ 14+2(i-1)\},$$
$$V_i = \{6+2(i-1),\ 7+2(i-1),\ 12+2(i-1)\},$$
$$W_i = \{8+2(i-1),\ 10+2(i-1),\ 13+2(i-1)\}.$$

なお，カークマンの女子学生問題はいろいろな形で拡張されており，15 人を $(6n+3)$ 人にして，毎日のグループ数 5 を $2n+1$ にして，7 日間を $(3n+1)$ 日間にした結果はよく知られている([論；28] 参照)．

定理 4.1.4 の証明 ………………………………

(1) ⇒ (2)　$D = (\Omega, \boldsymbol{B})$ を $2\text{-}(n^2+n+1, n+1, 1)$ デザインとする．D の 1 つのブロック B_0 をとり，次のように $\Omega', \boldsymbol{B}'$ を定める．

$$\Omega' = \Omega - B_0,$$
$$\boldsymbol{B}' = \{B - B_0 \mid B \in \boldsymbol{B},\ \ B \neq B_0\}.$$

このとき定理 4.1.5 により，$(\Omega', \boldsymbol{B}')$ は $2\text{-}(n^2, n, 1)$ デザインであることが分

かる．

(2) ⇒ (1)　$D = (\Omega, \boldsymbol{B})$ を $2\text{-}(n^2, n, 1)$ デザインとする．定理4.1.6により，D は

$$\boldsymbol{B} = \bigcup_{i=1}^{n+1} \{B_{i1}, B_{i2}, \cdots, B_{in}\}$$

$$\Omega = B_{i1} \cup B_{i2} \cup \cdots \cup B_{in} \qquad (\text{直和}) \quad (i = 1, 2, \cdots, n+1)$$

と表すことができる．そして，次のように $\Omega', \boldsymbol{B}'$ を定める．

$$\Omega' = \Omega \cup \{\infty_1, \infty_2, \cdots, \infty_{n+1}\}$$

$$\boldsymbol{B}' = \{B_{ij} \cup \{\infty_i\} \mid 1 \leqq i \leqq n+1,\ 1 \leqq j \leqq n\} \cup \{\{\infty_1, \infty_2, \cdots, \infty_{n+1}\}\}$$

このとき，$(\Omega', \boldsymbol{B}')$ は $2\text{-}(n^2+n+1, n+1, 1)$ デザインであることが分かる．

(3) ⇒ (2)　$A_1, A_2, \cdots, A_{n-1}$ を n 次ラテン方陣の完全直交系とし，それらの各成分からなる集合はどれも $\{1, 2, \cdots, n\}$ としてよい．いま，

$$\Omega = \{(i, j) \mid i = 1, 2, \cdots, n,\ \ j = 1, 2, \cdots, n\},$$

$$\boldsymbol{B} = \{U_i \mid i = 1, \cdots, n\} \cup \{V_i \mid i = 1, \cdots, n\}$$
$$\cup \{W_{ij} \mid i = 1, \cdots, n,\ \ j = 1, \cdots, n-1\},$$

$$U_i = \{(s, i) \mid s = 1, \cdots, n\},$$

$$V_i = \{(i, t) \mid t = 1, \cdots, n\},$$

$$W_{ij} = \{(s, t) \mid A_j \text{ の } (s, t) \text{ 成分} = i\}$$

とおく．このとき，

$$|\Omega| = n^2, \qquad |\boldsymbol{B}| = n^2 + n, \qquad \boldsymbol{B} \subseteqq \Omega^{(n)}$$

であり，$(\Omega, \boldsymbol{B})$ は $2\text{-}(n^2, n, 1)$ デザインであることがやさしく確かめられる．

(2) ⇒ (3)　$D = (\Omega, \boldsymbol{B})$ を $2\text{-}(n^2, n, 1)$ デザインとする．定理4.1.6により，D は

$$\boldsymbol{B} = \bigcup_{i=1}^{n+1} \{B_{i1}, B_{i2}, \cdots, B_{in}\}$$

$$\Omega = B_{i1} \cup B_{i2} \cup \cdots \cup B_{in} \qquad (\text{直和}) \quad (i = 1, 2, \cdots, n+1)$$

と表すことができる．そして，

$$U_j = B_{nj}, \qquad V_j = B_{n+1,j} \qquad (j = 1, 2, \cdots, n)$$

とおくと，任意の $U_i\,(1 \leqq i \leqq n)$ と $V_j\,(1 \leqq j \leqq n)$ に対して，$U_i \cap V_j$ は Ω

の1点 $\alpha(i,j)$ からなる集合となり，$\alpha(i,j)$ は (i,j) により一意的に定まる．

以上のもとで，$n-1$ 個の n 次行列 $A_1, A_2, \cdots, A_{n-1}$ を次のように定める（$i = 1, \cdots, n$，$j = 1, \cdots, n$）．

$$A_l \text{ の } (i,j) \text{ 成分} = k \Longleftrightarrow \alpha(i,j) \in B_{lk}$$

このとき，$A_1, A_2, \cdots, A_{n-1}$ は互いに直交するラテン方陣を表していることがやさしく確かめられる．

q を素数巾とするとき，$GF(q)$ 上の $PG(2,q)$ に関して次のことが成り立つ：点全部の個数は q^2+q+1，各直線に含まれる点の個数は $q+1$，相異なる任意の2点はただ1つの直線を決定する．したがって $PG(2,q)$ の点の集合を Ω，直線の集合を $\boldsymbol{B}$ とすると，$D = (\Omega, \boldsymbol{B})$ は 2-$(q^2+q+1, q+1, 1)$ デザインとなり，$PGL(3,q)$ が $\mathrm{Aut}(D)$ の部分群になることは明らかである．実際のところ**射影幾何の基本定理**（[和；8] 参照）で，$\mathrm{Aut}(D)$ は射影一般半線形群 $P\Gamma L(3,q)$ というものと一致することが知られている．

4.2　対称的デザイン

最初に 2-(v,k,λ) デザイン $D = (\Omega, \boldsymbol{B})$ に対し，D の**結合行列** A を次のように定める．

$$\Omega = \{\alpha_1, \alpha_2, \cdots, \alpha_v\}, \qquad \boldsymbol{B} = \{B_1, B_2, \cdots, B_b\}$$

とおくとき，A は v 行 b 列の行列で，

$$A \text{ の } (i,j) \text{ 成分} = \begin{cases} 1 & (\alpha_i \in B_j) \\ 0 & (\alpha_i \notin B_j). \end{cases}$$

一般に結合行列は，デザイン論ばかりでなく組合せ論の研究においては広く登場するものである．上で定めた A に対し，A とその転置行列 ${}^tA$ の積を考えると次の式を得る．

$$A^tA = \begin{pmatrix} r & \lambda & \lambda & \cdots & \lambda \\ \lambda & r & \lambda & \cdots & \lambda \\ \lambda & \lambda & \ddots & & \vdots \\ \vdots & \vdots & & \ddots & \lambda \\ \lambda & \lambda & \cdots & \lambda & r \end{pmatrix}$$

$$\det(A^tA) = (r+\lambda(v-1)) \begin{vmatrix} 1 & 1 & \cdots & \cdots & 1 \\ \lambda & r & \lambda & \cdots & \lambda \\ \lambda & \lambda & \ddots & & \vdots \\ \vdots & \vdots & & \ddots & \lambda \\ \lambda & \lambda & \cdots & \lambda & r \end{vmatrix}$$

$$= (r+\lambda(v-1)) \begin{vmatrix} 1 & 0 & \cdots & \cdots & 0 \\ \lambda & r-\lambda & 0 & \cdots & 0 \\ \lambda & 0 & \ddots & & \vdots \\ \vdots & \vdots & & \ddots & 0 \\ \lambda & 0 & \cdots & 0 & r-\lambda \end{vmatrix}$$

$$= (r-\lambda)^{v-1}(r+\lambda(v-1)).$$

ここで，

$$r+\lambda(v-1) = r+r(k-1) = rk$$

なので，D が自明でないならば，

$$\det(A^tA) \neq 0$$

が成り立つ．これが成り立つためには，

$$A \text{ の行数} \leqq A \text{ の列数}$$

でなくてはならないので，次の定理を得る．

定　理 | 4.2.1 ……………………………………………… **フィッシャーの不等式**

自明でない 2-(v, k, λ) デザインは

$$v \leqq b, \qquad r \geqq k$$

をみたす．

上の定理において，等号 $v = b$，すなわち $r = k$ が成り立つとき，2-デザインは**対称的**であるという．そこで，2-(v, k, λ) デザインが対称的ならば，結合

行列 A は正則である．このとき，I を v 次単位行列，J をすべての成分が 1 の v 次正方行列とすると，

$$\begin{aligned} {}^tAA &= A^{-1}(A{}^tA)A \\ &= A^{-1}((r-\lambda)I+\lambda J)A \\ &= (r-\lambda)I+\lambda A^{-1}JA \\ &= (r-\lambda)I+\lambda A^{-1}(kJ) \\ &= (r-\lambda)I+\lambda A^{-1}(AJ) \\ &= (k-\lambda)I+\lambda J \end{aligned}$$

が成り立つ．したがって D において，任意の異なる 2 つのブロックの共通集合は λ 個の点からなる集合となり，次の定理を得る．

定　理 | 4.2.2

2-(v,k,λ) デザイン $D=(\Omega,\boldsymbol{B})$ が対称的ならば，点とブロックの立場を入れ替えた組合せ構造 ${}^tD=(\boldsymbol{B},\Omega)$ も対称的 2-(v,k,λ) デザインとなる．ただし，D において点 α がブロック B の要素であるとき，またそのときに限って ${}^tD$ において点 B はブロック α の要素であると見なす．

一般の t-デザインの研究に関して，定理 4.1.2 から導かれる整数条件は，素朴ではあるものの役に立つことが多い．さらに対称的 2-デザインに関しては，その証明は省略するが([洋；1] 参照)，次の定理は強力である．

定　理 | 4.2.3 …………… **Bruck–Chowla–Ryser**

対称的 2-(v,k,λ) デザインが存在するならば，以下のことが成り立つ．

（1）　v が偶数のとき，$k-\lambda$ は平方数である．

（2）　v が奇数のとき，x,y,z に関する不定方程式

$$x^2=(k-\lambda)y^2+(-1)^{\frac{v-1}{2}}\lambda z^2$$

は，$x=y=z=0$ 以外の整数解をもつ．

対称的 2-デザインに関する議論を進める前に，補デザインの定義を行う．一般に t-(v,k,λ) デザイン $D=(\Omega,\boldsymbol{B})$ に対し，

$$\bar{D} = (\Omega, \bar{\boldsymbol{B}}), \qquad \bar{\boldsymbol{B}} = \{\Omega - B \mid B \in \boldsymbol{B}\}$$

と定めると，それは $v \geqq t+k$ のとき t-デザインとなり，D の**補デザイン**という．実際，Ω の相異なる任意の t 点 $\alpha_1, \alpha_2, \cdots, \alpha_t$ に対し，$\{\alpha_1, \alpha_2, \cdots, \alpha_t\}$ と共通部分をもたない D のブロックの個数は

$$\begin{aligned}
&|\boldsymbol{B}| - |\{(\alpha_i, B) \mid 1 \leqq i \leqq t,\ B \in \boldsymbol{B},\ \alpha_i \in B\}| \\
&\quad + |\{(\{\alpha_i, \alpha_j\}, B) \mid 1 \leqq i < j \leqq t,\ B \in \boldsymbol{B},\ \alpha_i, \alpha_j \in B\}| \\
&\quad - \quad \cdots\cdots \\
&\quad + (-1)^t |\{(\{\alpha_1, \alpha_2, \cdots, \alpha_t\}, B) \mid B \in \boldsymbol{B},\ \alpha_1, \alpha_2, \cdots, \alpha_t \in B\}| \\
&= \lambda_0 - \binom{t}{1}\lambda_1 + \binom{t}{2}\lambda_2 - \binom{t}{3}\lambda_3 + \cdots + (-1)^t \binom{t}{t}\lambda_t
\end{aligned}$$

である．なぜならば，$B \cap \{\alpha_1, \alpha_2, \cdots, \alpha_t\} = \emptyset$ となる D のブロック B は上式の第 1 項で 1 回だけ計算されており，

$$|B \cap \{\alpha_1, \alpha_2, \cdots, \alpha_t\}| = r \qquad (1 \leqq r \leqq t)$$

となる D のブロック B は上式で何回計算されているかを数えると，第 1 項で 1 回，第 2 項で r 回，第 3 項で $\binom{r}{2}$ 回，…，第 r 項で $\binom{r}{r}$ 回それぞれ計算されている．そして，

$$\sum_{i=0}^{r} (-1)^i \binom{r}{i} = (1-1)^r = 0$$

なので，結局この場合の B はプラスマイナスの符合を加味すると 0 回だけ計算されていることになる．

以上から，$\bar{D} = (\Omega, \bar{\boldsymbol{B}})$ は

$$t\text{-}\left(v, v-k, \sum_{i=0}^{t} (-1)^i \binom{t}{i} \lambda_i\right)$$

デザインとなる．

対称的 2-デザインの研究において，とくに注目される対象は射影平面とアダマール型のデザインというものである．**位数** n **のアダマール型のデザイン**とは対称的 2-$(4n-1, 2n-1, n-1)$ デザインのことであり，「2 以上のすべての自然数 n に対して，位数 n のアダマール型のデザインは存在する」という予想は

有名である．ちなみに，$n \leqq 106$ ではすべて背定的に解決しているが，最近 IPM (Institute for Studies in Theoretical Physics and Mathematics) の計算センターで $n=107$ の場合を発見したようである．なお多くの人達にとっては，アダマール型のデザインとその存在性が同値である $4n$ 次のアダマール行列の方に関心が高い．アダマール行列の研究に関する様々な結果は，［論；30］によくまとめられている．

定　理｜4.2.4

自明でない対称的 2-(v,k,λ) デザイン D に対し，$n=k-\lambda$ とおくと

$$4n-1 \leqq v \leqq n^2+n+1$$

が成り立つ．ここで，もし $v=n^2+n+1$ ならば，D は位数 n の射影平面であるか，またはその補デザインである．また，もし $v=4n-1$ ならば，D は位数 n のアダマール型のデザインであるか，またはその補デザインである．

証　明

$D=(\Omega,\boldsymbol{B})$ とおく．もし $k=v-1$ ならば，D の任意の点 α に対し，α を含むブロックの個数は一定であることから，$\Omega-\{\alpha\}\in\boldsymbol{B}$ でなくてはならない．したがってこの場合，D は自明なデザインになる．そこで，仮定より $k\leqq v-2$ となり，D の補デザイン $\bar{D}$ が定義できる．いま，$\bar{D}$ を 2-$(v,v-k,\bar{\lambda})$ デザインとすると，

$$\begin{aligned}\bar{\lambda}&=\lambda_0-2\lambda_1+\lambda\\&=v-2k+\lambda\end{aligned}$$

である．さて，

$$\begin{aligned}\lambda+\bar{\lambda}&=v-2k+2\lambda=v-2n,\\ \lambda\bar{\lambda}&=\lambda(v-2k+\lambda)\\&=\lambda v-2k\lambda+\lambda^2\\&=k(k-1)+\lambda-2k\lambda+\lambda^2\\&=(k-\lambda)^2-k+\lambda=n(n-1)\end{aligned}$$

である．よって，

$$(\lambda+\bar{\lambda})^2 \geqq 4\lambda\bar{\lambda} = 4n(n-1)$$

を得るが，$n \geqq 2$ ならば $4n(n-1)$ は平方数にならない．したがって，

$$(v-2n)^2 = (\lambda+\bar{\lambda})^2 \geqq 4n(n-1)+1 = (2n-1)^2$$

$$v \geqq 2n+2n-1 = 4n-1$$

が成り立つ．一方，$\bar{\lambda} \geqq 1$ より

$$v-2k+\lambda-1 = v-2(n+\lambda)+\lambda-1 = v-2n-\lambda-1 \geqq 0$$

である．よって，

$$(\lambda-1)(v-2k+\lambda-1) \geqq 0$$

$$(\lambda-1)(v-2k+\lambda)-(\lambda-1) \geqq 0$$

$$\lambda(v-2k+\lambda)-(v-2k+\lambda+\lambda-1) \geqq 0$$

$$\lambda\bar{\lambda}-(v-2n-1) \geqq 0$$

$$v \leqq n(n-1)+2n+1 = n^2+n+1$$

が成り立つ．以上から，定理の前半が示せたことになる．

次に，$v = n^2+n+1$ とすると

$$v-2n-1 = n^2-n = \lambda\bar{\lambda} = \lambda(v-2n-\lambda)$$
$$= \lambda(v-2n-1)-\lambda(\lambda-1),$$

$$(\lambda-1)(v-2n-1-\lambda) = 0$$

となるので，$\lambda = 1$ または $\lambda = v-2n-1$ を得る．もし $\lambda = 1$ ならば，

$$k(k-1) = \lambda(v-1) = v-1 = n(n+1)$$

から $k = n+1$ となり，D は位数 n の射影平面になる．また，もし $\lambda = v-2n-1$ ならば，

$$k(k-1) = \lambda(v-1) = (n^2-n)(n^2+n) = n^2(n^2-1)$$

から $k = n^2$ となり，D は位数 n の射影平面の補デザインになる．

最後に，$v = 4n-1$ とすると

$$k(k-1) = \lambda(4n-2) = 2\lambda(2n-1) = 2(k-n)(2n-1),$$

$$(k-2n)(k-2n+1) = k^2-k(4n-1)+2n(2n-1)$$
$$= k^2-k-k(4n-2)+2n(2n-1) = 0$$

となるので，$k = 2n$ または $k = 2n-1$ を得る．もし $k = 2n-1$ ならば，

$$\lambda(v-1) = k(k-1) = (2n-1)(2n-2)$$

から $\lambda = n-1$ となり，D は位数 n のアダマール型のデザインになる．また，もし $k = 2n$ ならば，

$$\lambda(v-1) = k(k-1) = 2n(2n-1)$$

から $\lambda = n$ となり，D は位数 n のアダマール型のデザインの補デザインになる．

例 4.2.5

n を自然数，q を素数巾とするとき，$PG(n,q)$ の点全体からなる集合を Ω，$PG(n,q)$ の $d\ (\geqq 1)$ 次元部分空間全体からなる集合を $\boldsymbol{B}$ とおけば，$(\Omega, \boldsymbol{B})$ は次のパラメーターをみたす 2-(v,k,λ) デザインになる．

$$v = \frac{q^{n+1}-1}{q-1}, \qquad k = \frac{q^{d+1}-1}{q-1},$$

$$\lambda = \frac{(q^{n-1}-1)(q^{n-2}-1)\cdots(q^{n-d+1}-1)}{(q^{d-1}-1)(q^{d-2}-1)\cdots(q-1)}.$$

実際，$GF(q)$ 上の $n+1$ 次元線形空間において，1 次独立な 2 つのベクトル $\boldsymbol{u}_1, \boldsymbol{u}_2$ に対し，$\boldsymbol{u}_1$ と $\boldsymbol{u}_2$ を含む $d+1$ 次元部分空間の個数は

$$\frac{(q^{n+1}-q^2)(q^{n+1}-q^3)\cdots(q^{n+1}-q^d)}{(q^{d+1}-q^2)(q^{d+1}-q^3)\cdots(q^{d+1}-q^d)}$$

$$= \frac{(q^{n-1}-1)(q^{n-2}-1)\cdots(q^{n-d+1}-1)}{(q^{d-1}-1)(q^{d-2}-1)\cdots(q-1)}$$

である．

とくに，$d = n-1$，$q = 2$ のとき，

$$v = 2^{n+1}-1, \qquad k = 2^n-1, \qquad \lambda = 2^{n-1}-1$$

となるが，これは $(\Omega, \boldsymbol{B})$ が位数 2^{n-1} のアダマール型のデザインであることを意味している．

4.3 タイトデザイン

本節では [論；29] にしたがって，4.2 節で述べたフィッシャーの不等式を拡張し，タイトデザインを導入することを目標にする．

定理 | 4.3.1

$D=(\Omega,\boldsymbol{B})$ を t-(v,k,λ) デザインとし，i,j を $i,j\geqq 0$，$i+j\leqq t$ をみたす整数とする．このとき，

$$|I|=i,\quad |J|=j,\quad I\cap J=\varnothing$$

をみたす Ω の部分集合 I,J に対し，

$$b_i^j=|\{B\in\boldsymbol{B}\mid B\supseteqq I,\ B\cap J=\varnothing\}|$$

とおくと，

$$b_i^j=\frac{\binom{v-i-j}{k-i}\lambda}{\binom{v-t}{k-t}}$$

である．とくに，b_i^j は I,J のとり方によらない数である．

証明

最初に，4.2 節で補デザインを導入したときと同様な論法を用いて，

$$b_i^j=\sum_{r=0}^{j}(-1)^r\binom{j}{r}\lambda_{i+r}$$
$$=\lambda\left(\sum_{r=0}^{j}(-1)^r\binom{j}{r}\frac{\binom{v-i-r}{t-i-r}}{\binom{k-i-r}{t-i-r}}\right)$$

が成り立つ．ここで上式は，$\boldsymbol{B}=\Omega^{(k)}$ である自明なデザインでも成り立つことに留意すると，その場合には

$$\lambda=\binom{v-t}{k-t},\qquad b_i^j=\binom{v-i-j}{k-i}$$

である．したがって，

$$\sum_{r=0}^{j}(-1)^r\binom{j}{r}\frac{\binom{v-i-r}{t-i-r}}{\binom{k-i-r}{t-i-r}}=\frac{\binom{v-i-j}{k-i}}{\binom{v-t}{k-t}}$$

を得る(上式は自明なデザインに限定するものでない).

定 理 | 4.3.2

$D=(\Omega,\boldsymbol{B})$ を $t=2s$ (s は自然数), $v \geqq k+s$ をみたす t-(v,k,λ) デザインとすると

$$b \geqq \binom{v}{s}$$

が成り立つ.

証 明

$\Omega^{(s)}$ を基底とする実数体 $\boldsymbol{R}$ 上の線形空間を V とし, $\boldsymbol{B}$ の各元 B に対し

$$\hat{B}=\sum_{\substack{S\in\Omega^{(s)}\\ S\subseteqq B}} S$$

とおく. このとき, $\{\hat{B}\mid B\in\boldsymbol{B}\}$ が V を生成することを示せば証明は完成する.

いま $\Omega^{(s)}$ の任意の1つの元 S_0 をとり, それを固定する. 各 $i=0,1,\cdots,s$ に対し

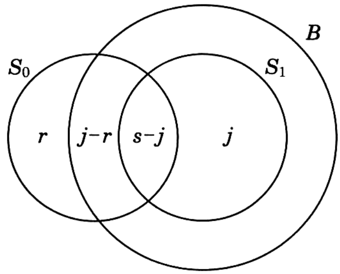
$$E_i=\sum_{\substack{S\in\Omega^{(s)}\\ |S\cap S_0|=s-i}} S, \qquad F_i=\sum_{\substack{B\in\boldsymbol{B}\\ |B\cap S_0|=s-i}} \hat{B}$$

とおく. ここで, $E_0=S_0$ に留意する. 次に $\Omega^{(s)}$ の任意の元 S_1 をとり, $|S_1\cap S_0|=s-j$ とすると, 各 $r=0,1,\cdots,s$ に対し

$$\begin{aligned} F_r \text{ における } S_1 \text{ の係数} &= |\{B\in\boldsymbol{B}\mid |B\cap S_0|=s-r,\ S_1\subseteqq B\}| \\ &= \begin{cases} |\{B\in\boldsymbol{B}\mid |B\cap(S_0-S_1)|=j-r, \\ \quad S_1\subseteqq B\}| \quad (j\geqq r \text{ のとき}) \\ 0 \quad (j<r \text{ のとき}) \end{cases} \\ &= \binom{j}{r} b^r_{s+j-r} \end{aligned}$$

を得る. なお, $0\leqq j<r$ のとき $\binom{j}{r}=0$ である. よって,

$$F_r=\sum_{i=r}^{s}\binom{i}{r} b^r_{s+i-r} E_i \qquad (r=0,1,\cdots,s)$$



$$\begin{pmatrix} F_0 \\ F_1 \\ \vdots \\ \vdots \\ F_s \end{pmatrix} = \begin{pmatrix} & & \\ & \binom{i}{r} b^r_{s+i-r} & \\ & & \end{pmatrix} \begin{pmatrix} E_0 \\ E_1 \\ \vdots \\ \vdots \\ E_s \end{pmatrix}$$

が成り立つ．ここで上式右辺の最初の行列は，(r, i) 成分が $\binom{i}{r} b^r_{s+i-r}$ となる $s+1$ 次の上三角行列で($r=0, 1, \cdots, s$，$i=0, 1, \cdots, s$)，定理 4.3.1 より対角成分はどれも 0 でない．したがってそれは正則となるので，

$$E_0, E_1, \cdots, E_s \in \langle F_0, F_1, \cdots, F_s \rangle \subseteqq \langle \hat{B} \mid B \in \boldsymbol{B} \rangle$$

を得る．ただし，$\langle F_0, F_1, \cdots, F_s \rangle$ は $F_0, F_1, \cdots, F_s$ で生成された V の部分空間である．よって，$S_0 = E_0$ は $\langle \hat{B} \mid B \in \boldsymbol{B} \rangle$ の元となり，$\Omega^{(s)}$ の任意の元は $\langle \hat{B} \mid B \in \boldsymbol{B} \rangle$ の元である．

上定理において $b = \binom{v}{s}$ が成り立つとき，D を**タイト** t-(v, k, λ) デザインという．

定　理 | 4.3.3

Ω を v 個の元からなる集合とし，X を次の条件をみたす $\Omega^{(k)}$ の部分集合とする．

$$k > \mu_1 > \mu_2 > \cdots > \mu_s \geqq 0$$

となる $s\,(\geqq 1)$ 個の整数 $\mu_1, \mu_2, \cdots, \mu_s$ があって，X の任意の 2 つの元 $A \neq B$ に対し，

$$|A \cap B| \in \{\mu_1, \mu_2, \cdots, \mu_s\}$$

をみたすとする．このとき，

$$|X| \leqq \binom{v}{s}.$$

証 明

X を基底とする $\boldsymbol{R}$ 上の線形空間を V とし，$\Omega^{(s)}$ の各元 S に対し

$$\bar{S} = \sum_{\substack{A \in X \\ A \supseteqq S}} A$$

とおく．このとき，$\{\bar{S} \mid S \in \Omega^{(s)}\}$ が V を生成することを示せば証明は完成する．

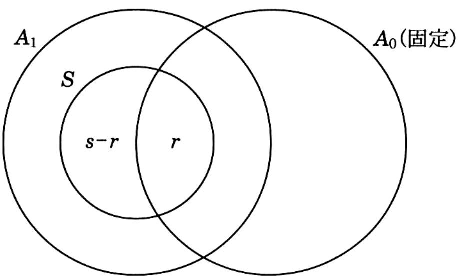
$\mu_0 = k$ とおき，X の任意の元 A_0 をとり，それを固定する．各 $i = 0, 1, \cdots, s$ に対し

$$G_i = \sum_{\substack{S \in \Omega^{(s)} \\ |S \cap A_0| = i}} \bar{S}, \qquad H_i = \sum_{\substack{A \in X \\ |A \cap A_0| = \mu_i}} A$$

とおく．ここで，$H_0 = A_0$ に留意する．次に X の任意の元 A_1 をとり，$|A_1 \cap A_0| = \mu_j$ とすると，各 $r = 0, 1, \cdots, s$ に対し

$$G_r \text{ における } A_1 \text{ の係数} = |\{S \in \Omega^{(s)} \mid |S \cap A_0| = r,\ S \subseteqq A_1\}|$$
$$= \binom{\mu_j}{r}\binom{k - \mu_j}{s - r}$$

を得る．よって，



$$G_r = \sum_{i=0}^{s} \binom{\mu_i}{r}\binom{k-\mu_i}{s-r} H_i \quad (r = 0, 1, \cdots, s)$$

$$\begin{pmatrix} G_0 \\ G_1 \\ \vdots \\ \vdots \\ G_s \end{pmatrix} = \begin{pmatrix} & & \\ & \binom{\mu_i}{r}\binom{k-\mu_i}{s-r} & \\ & & \end{pmatrix} \begin{pmatrix} H_0 \\ H_1 \\ \vdots \\ \vdots \\ H_s \end{pmatrix}$$

が成り立つ．ここで上式右辺の最初の行列は，(r, i) 成分が $\binom{\mu_i}{r}\binom{k-\mu_i}{s-r}$ となる $s+1$ 次行列である $(r = 0, 1, \cdots, s,\ \ i = 0, 1, \cdots, s)$．もし，それが正則であることが分かれば，

$$A_0 = H_0 \in \langle G_0, G_1, \cdots, G_s \rangle \subseteqq \langle \bar{S} \mid S \in \Omega^{(s)} \rangle$$

となって，証明は完成することになる．そこで，その行列の第 i 行ベクトルを $\boldsymbol{u}_i$ とおき，$\boldsymbol{u}_0, \boldsymbol{u}_1, \cdots, \boldsymbol{u}_s$ が1次独立になることを示そう．

いま，$\boldsymbol{R}$ の元 $c_0, c_1, \cdots, c_s$ に対し，

$$c_0\boldsymbol{u}_0 + c_1\boldsymbol{u}_1 + \cdots + c_s\boldsymbol{u}_s = \boldsymbol{0} \qquad \text{(零ベクトル)}$$

とすると，x の多項式

$$f(x) = \sum_{m=0}^{s} c_m \binom{x}{m}\binom{k-x}{s-m}$$

は相異なる $s+1$ 個の根 $\mu_0, \mu_1, \cdots, \mu_s$ をもつ．なお，

$$\binom{x}{m} = \frac{x(x-1)\cdots(x-m+1)}{m!}$$

である．ところが $f(x)$ は x の s 次多項式なので，

$$f(x) \equiv 0$$

でなくてはならない．したがって，

$$f(0) = c_0\binom{k}{s} = 0$$

から $c_0 = 0$ を得る．そして，

$$f(1) = c_1\binom{k-1}{s-1} = 0$$

から $c_1 = 0$ を得る．以下同様にして，

$$c_0 = c_1 = c_2 = \cdots\cdots = c_s = 0$$

となることが分かる.

定 理 | 4.3.4

$D = (\Omega, \boldsymbol{B})$ を，$t = 2s$ (s は自然数)，$v \geqq k+s$ をみたす t-(v, k, λ) デザインとすると,

$$|\{|A \cap B| \mid A \neq B \in \boldsymbol{B}\}| \geqq s$$

が成り立つ．さらに，上不等式の等号が成立するためには，D がタイト t-(v, k, λ) デザインであることが必要十分条件である.

証 明

前半は定理 4.3.2 と定理 4.3.3 より明らかである．また後半の必要性も，同じく明らかである．後半の十分性を示すために，タイト t-(v, k, λ) デザイン D に対し，0 以上 k より小の相異なる s 個の整数 $\mu_1, \mu_2, \cdots, \mu_s$ があって，どの 2 つのブロック $A \neq B$ も必ず

$$|A \cap B| \in \{\mu_1, \mu_2, \cdots, \mu_s\}$$

をみたすことをいえばよい.

定理 4.3.2 の証明と同じ記法を用いると，$b = \binom{v}{s}$ 個のベクトル $\{\widehat{B} \mid B \in \boldsymbol{B}\}$ は $V = \langle \Omega^{(s)} \rangle$ の基底である．いま，任意の 1 つのブロック A_0 を固定し，すべてのブロック B に対し

$$\mu_B = |B \cap A_0|$$

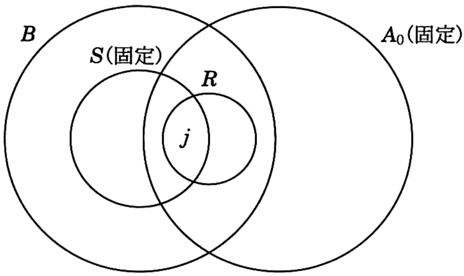
とおく．各 $i = 0, 1, \cdots, s$ に対し

$$M_i = \sum_{\substack{S \in \Omega^{(s)} \\ |S \cap A_0| = i}} S, \qquad N_i = \sum_{B \in \boldsymbol{B}} \binom{\mu_B}{i} \widehat{B}$$

とおく．いま，$|S \cap A_0| = i$ となる $S \in \Omega^{(s)}$ と i を固定して考えると,

N_r における S の係数

$$= \sum_{\substack{B \in \boldsymbol{B} \\ B \supseteq S}} \binom{\mu_B}{r}$$



$$= |\{(B, R) \in \boldsymbol{B} \times \Omega^{(r)} \mid B \supseteqq S,\ \ R \subseteqq A_0 \cap B\}|$$

が分かる．そして，

$$|R| = r \geqq j = |R \cap S|, \qquad R \subseteqq A_0.$$

をみたす集合 R のとり方の総数は $\binom{i}{j}\binom{k-i}{r-j}$ で，その各々の R に対し，

$$|\{B \in \boldsymbol{B} \mid B \supseteqq S, R \subseteqq A_0 \cap B\}| = \lambda_{s+r-j}$$

となる．よって，

$$N_r \text{ における } S \text{ の係数} = \sum_{j=0}^{i} \binom{i}{j}\binom{k-i}{r-j} \lambda_{s+r-j}$$

が成り立つ．上式の右辺を c_r^i とおくと，c_r^i は v, k, s, λ, i, r によって定まる定数で，

$$N_r = \sum_{i=0}^{s} c_r^i M_i$$

を得る．ここで上式は，$r = 0, 1, \cdots, s$ に対して成り立つので，

$$\{N_r - c_r^s M_s \mid r = 0, 1, \cdots, s\} \subseteqq \langle M_0, M_1, \cdots, M_{s-1} \rangle.$$

したがって，$s+1$ 個の元 $N_r - c_r^s M_s\ (r = 0, 1, \cdots, s)$ は，V において1次従属となる．よって，$(a_0, a_1, \cdots, a_s) \neq (0, 0, \cdots, 0)$ となる $\boldsymbol{R}$ の元 $a_0, a_1, \cdots, a_s$ があって，

$$\sum_{r=0}^{s} a_r (N_r - c_r^s M_s) = \mathbf{0} \qquad (\text{零ベクトル}),$$

$$\sum_{r=0}^{s} a_r \left(\sum_{B \in \boldsymbol{B}} \binom{\mu_B}{r} \widehat{B} - c_r^s \widehat{A}_0 \right) = \mathbf{0},$$

$$\sum_{\substack{B \in \boldsymbol{B} \\ B \neq A_0}} \left(\sum_{r=0}^{s} a_r \binom{\mu_B}{r} \right) \widehat{B} + \sum_{r=0}^{s} a_r \left(\binom{k}{r} - c_r^s \right) \widehat{A}_0 = \boldsymbol{0}$$

となる．ここで，$\{\widehat{B} \mid B \in \boldsymbol{B}\}$ は V の基底なので，$B \neq A_0$ に関して

$$\sum_{r=0}^{s} a_r \binom{\mu_B}{r} = 0$$

でなくてはならない．すなわち，$\mu_B\ (B \neq A_0)$ は s 次多項式

$$f(x) = \sum_{r=0}^{s} a_r \binom{x}{r}$$

の根になる．ところが，$f(x)$ の各係数は A_0 のとり方には無関係である．それゆえ，D の相異なる 2 つのブロック B_1, B_2 に対し，$|B_1 \cap B_2|$ は s 次多項式 $f(x)$ の根である．

明らかに，対称的 2-デザインはタイトデザインである．また，$D = (\Omega, \boldsymbol{B})$ を $|\Omega| = v$，$\boldsymbol{B} = \Omega^{(v-s)}$ となる自明な $2s$-デザインとすると，定理 4.3.4 により D はタイトデザインになる．1979 年には次の結果が証明され，最近はタイトデザインを拡張したものが多項式空間という世界で研究されている([洋；13] 参照)．

定　理 | 4.3.5 ……………………(Enomoto, Ito, Noda[論；11], Bremner[論；7])

D を自明でないタイト 4-デザインとすると，D はウィットシステム W_{23}(4-(23, 7, 1)デザイン)かその補デザインである．

4.4　デザインの軌道行列

デザインの研究では，多重可移置換群のような大きい群ではなく，小さい群がその自己同型群として作用している場合がよくある．実際，小さい群が作用しているデザインについての論文はたくさん出ているが，研究全般を動かすような結果はまだ少ないようである．しかしながら，その方面に関心をもつと，必ずと言っていいほど軌道行列という道具が登場する．本節では個々の分類結果を紹介するのでなく，他分野にも応用可能な軌道行列の考え方を紹介しよう．

以下述べるように，それはいくつもの整数の不定方程式を導くのである．

$D=(\Omega,\boldsymbol{B})$ を 2-(v,k,λ) デザインとし， G を $\mathrm{Aut}(D)$ の部分群とする．そして，Ω 上の G-軌道全体を $X_1, X_2, \cdots, X_m$ とし，$\boldsymbol{B}$ 上の G-軌道全体を $Y_1, Y_2, \cdots, Y_n$ とする．このとき，次のように定めた (m,n) 型の行列 $A=(a_{ij})$ を G に関する D の**軌道行列**という．

B を Y_j の元とするとき，A の (i,j) 成分 a_{ij} は

$$a_{ij}=|X_i\cap B|$$

で与えられる．また，

$$x_i=|X_i| \qquad (1\leqq i\leqq m), \qquad y_j=|Y_j| \qquad (1\leqq j\leqq n)$$

とおく．最初に，以下の集合の元の個数をそれぞれ2通りに求めることから(B を先に定めるか後に定めるか)，順に3つの等式(1)，(2)，(3)が導かれる．

$$\{(\delta,B)\,|\,\delta\in X_i,\ \delta\in B,\ B\in\boldsymbol{B}\},$$
$$\{(\delta,\delta',B)\,|\,\delta,\delta'\in X_i,\ \delta\neq\delta',\ \delta,\delta'\in B,\ B\in\boldsymbol{B}\},$$
$$\{(\delta,\eta,B)\,|\,\delta\in X_c,\ \eta\in X_d,\ \delta,\eta\in B,\ B\in\boldsymbol{B}\} \qquad (c<d).$$

(1)　$$\sum_{j=1}^{n}a_{ij}y_j=x_ir \qquad (1\leqq i\leqq m)$$

(2)　$$\sum_{j=1}^{n}a_{ij}(a_{ij}-1)y_j=x_i(x_i-1)\lambda \qquad (1\leqq i\leqq m)$$

(3)　$$\sum_{j=1}^{n}a_{cj}a_{dj}y_j=x_cx_d\lambda \qquad (1\leqq c<d\leqq m)$$

次に，G を素数位数 p の巡回群とすると，x_i と y_j は p または1となる．もし B が G の作用によって固定されるブロックとすると，すべての $i\,(1\leqq i\leqq m)$ に対し $X_i\cap B=\emptyset$ あるいは $X_i\subseteqq B$ のどちらかが成り立つ．いま，$|X_i|=p$ となる X_i に対して

$$u_i=|\{B\in\boldsymbol{B}\,|\,X_i\subseteqq B,\ (B)G=B\}|$$

とおき，$|X_c|=|X_d|=p\ (c<d)$ となる X_c, X_d に対して

$$u_{cd}=|\{B\in\boldsymbol{B}\,|\,X_c\subseteqq B,\ X_d\subseteqq B,\ (B)G=B\}|$$

とおいて考えてみる．まず，(1)，(2)，(3)から次の3つの等式を順に得る．

$$\sum_{y_j=1\text{ となる }j}a_{ij}+\sum_{y_j=p\text{ となる }j}a_{ij}p=pr,$$

$$\sum_{y_j=1\text{となる}j} a_{ij}(a_{ij}-1)+\sum_{y_j=p\text{となる}j} a_{ij}(a_{ij}-1)p = p(p-1)\lambda,$$

$$\sum_{y_j=1\text{となる}j} a_{cj}a_{dj}+\sum_{y_j=p\text{となる}j} a_{cj}a_{dj}p = p\cdot p\lambda.$$

したがって，下記の3つの等式が成り立つ.

(4) $\displaystyle\sum_{y_j=p\text{となる}j} a_{ij} = r-u_i$

(5) $\displaystyle\sum_{y_j=p\text{となる}j} a_{ij}(a_{ij}-1) = (p-1)(\lambda-u_i)$

(6) $\displaystyle\sum_{y_j=p\text{となる}j} a_{cj}a_{dj} = p(\lambda-u_{cd})$

4.5 アソシエーションスキームとウィットシステム

5章で紹介する距離正則グラフもそうであるが，アソシエーションスキームの概念をもつ組合せ構造の研究は，いわゆる代数的組合せ論の中心的課題である．本節では，アソシエーションスキームの定義，例および簡単な性質を述べ，最後にその立場からウィットシステムを特徴付けた結果を紹介する．

X を有限集合とし，$X^{(2)}$ が以下の2条件をみたす d 個の空でない部分集合 $\Gamma_1, \Gamma_2, \cdots, \Gamma_d$ の直和として表されるとき，$(X, \{\Gamma_i \mid 1 \leqq i \leqq d\})$ を**クラス d のアソシエーションスキーム**という．

(1) X の元 x に対し，

$$n_i(x) = |\{y \in X \mid \{x, y\} \in \Gamma_i\}|$$

は i のみによって定まり，x のとり方によらない $(i=1,2,\cdots,d)$．

(2) $\{x, y\} \in \Gamma_h$ となる X の異なる元 x, y に対し，

$$p_{ij}^h(x, y) = |\{z \in X \mid \{x, z\} \in \Gamma_i,\ \{z, y\} \in \Gamma_j\}|$$

は i, j, h のみによって定まり，x と y のとり方によらない $(i, j, h \in \{1, 2, \cdots, d\})$．

上の定義から以後，$n_i(x)$ を n_i，$p_{ij}^h(x, y)$ を p_{ij}^h で表すことにする．X の異なる2元 x, y が $\{x, y\} \in \Gamma_i$ をみたすとき，x と y は Γ_i の関係にあるという．また，便宜上

$$n_0 = 1, \quad p_{ii}^0 = n_i, \quad p_{0i}^i = p_{i0}^i = 1,$$
$$p_{ij}^0 = 0\,(i \neq j), \quad p_{0j}^h = 0\,(h \neq j), \quad p_{i0}^h = 0\,(i \neq h)$$

と定める．そして，X のすべての元 x はそれ自身と Γ_0 の関係にあるとする．

例 4.5.1

（ア）Ω を v 個の元からなる集合とし，k を $k \leqq \dfrac{v}{2}$ をみたす自然数とする．このとき $\Delta = \Omega^{(k)}$ の異なる 2 元 X, Y に対し，

$$\{X, Y\} \in \Gamma_i \Longleftrightarrow |X \cap Y| = k-i$$

と定めることにより，クラス k のアソシエーションスキームを得る．実際，

$$\Delta^{(2)} = \Gamma_1 \cup \Gamma_2 \cup \cdots \cup \Gamma_k \qquad (\text{直和})$$

となり，Ω 上の対称群 S^{Ω} は Δ 上に作用し，その作用を考えることにより，条件(1)，(2)の成立が分かる．なぜならば，

$$\{X, Y\},\ \{X', Y'\} \in \Gamma_i$$

とすると，

$$X^g = X', \qquad Y^g = Y'$$

となる $g \in S^{\Omega}$ が存在するからである．一般に，このような型のアソシエーションスキームを**ジョンソンスキーム** $J(v, k)$ という．

（イ）n を自然数，q を 2 以上の整数，Q を q 個の元からなる集合とする．このとき，

$$V = \{(x_1, x_2, \cdots, x_n) \mid x_i \in Q\}$$

の異なる 2 元 $X = (x_1, x_2, \cdots, x_n)$，$Y = (y_1, y_2, \cdots, y_n)$ に対し，

$$\{X, Y\} \in \Gamma_i \Longleftrightarrow |\{j \mid x_j \neq y_j,\ 1 \leqq j \leqq n\}| = i$$

と定めることにより，クラス n のアソシエーションスキームを得る．実際，

$$V^{(2)} = \Gamma_1 \cup \Gamma_2 \cup \cdots \cup \Gamma_n \qquad (\text{直和})$$

となり，以下述べる群 G は V 上に作用し，その作用を考えることにより条件(1)，(2)の成立は(ア)と同様にして分かる．一般に，このような型のアソシエーションスキームを**ハミングスキーム** $H(n, q)$ という．

Ω を $\{1, 2, \cdots, n\}$ とし，n 個の S^Q（Q 上の対称群）と 1 個の S^{Ω}（Ω 上の対称群）の直積集合

$$\{(a_1, a_2, \cdots, a_n, b) \mid a_i \in S^Q (1 \leqq i \leqq n),\ \ b \in S^\Omega\}$$

を G とし，G の任意の元 $g = (a_1, a_2, \cdots, a_n, b)$ と V の任意の元 $X = (x_1, x_2, \cdots, x_n)$ に対し，X は g によって次の $Y = (y_1, y_2, \cdots, y_n)$ に移されるものとする．

$$y_i = (x_{(i)b^{-1}})^{a_{(i)b^{-1}}} \qquad (i = 1, 2, \cdots, n)$$

明らかに G は V 上の置換群であり，それを S^Q と S^Ω の**レス積**という．なお**レス積**は，一般に S^Q の部分群と S^Ω の部分群に対して同様に定義できる．

（ウ） G を有限集合 Ω $(|\Omega| \geqq 2)$ 上のランク r の可移置換群とすると，G は自然な作用で $\Omega \times \Omega = \{(\alpha, \beta) \mid \alpha, \beta \in \Omega\}$ 上の置換群となり，$\Omega \times \Omega$ は G-軌道 $\Delta_0 = \{(\alpha, \alpha) \mid \alpha \in \Omega\}$, Δ_1, $\cdots$, Δ_{r-1} によって，

$$\Omega \times \Omega = \Delta_0 \cup \Delta_1 \cup \cdots \cup \Delta_{r-1} \qquad (\text{直和})$$

と表せる．いま，

$${}^t\Delta_i = \{(\beta, \alpha) | (\alpha, \beta) \in \Delta_i\} \qquad (i = 0, 1, \cdots, r-1)$$

とおくと，${}^t\Delta_0 = \Delta_0$ であり，${}^t\Delta_i$ はある Δ_j になる．もし ${}^t\Delta_i = \Delta_i$ $(i = 1, 2, \cdots, r-1)$ が成り立つならば，

$$\Gamma_i = \{\{\alpha, \beta\} \in \Omega^{(2)} | (\alpha, \beta) \in \Delta_i\} \qquad (i = 1, 2, \cdots, r-1)$$

とおくことにより，

$$\Omega^{(2)} = \Gamma_1 \cup \Gamma_2 \cup \cdots \cup \Gamma_{r-1} \qquad (\text{直和})$$

と表せる．そして，この直和分割によってクラス $r-1$ のアソシエーションスキームを得る．実際，各 Γ_i と各 $\alpha \in \Omega$ に対し，

$$\Gamma_i(\alpha) = \{\gamma \in \Omega | \{\alpha, \gamma\} \in \Gamma_i\}$$

とおくと，$\Gamma_i(\alpha)$ は G_α の $\Omega - \{\alpha\}$ 上の軌道である．さらに，G の任意の元 g に対し，$(\Gamma_i(\alpha))g$ は $g^{-1}G_\alpha g = G_{\alpha^g}$ の軌道である．ここで $\{(\alpha^g, \beta^g) | \beta \in \Gamma_i(\alpha)\} \subseteqq \Gamma_i$ なので，

$$(\Gamma_i(\alpha))g = \Gamma_i(\alpha^g)$$

が成り立つ．したがって G の作用を考えることにより，条件(1)，(2)の成立は(ア)と同様にして分かる．

とくに，$|\Delta_1|, |\Delta_2|, \cdots, |\Delta_{r-1}|$ がすべて異なるときは，明らかに

$${}^t\Delta_i = \Delta_i \qquad (i = 1, 2, \cdots, r-1)$$

が成り立つことに留意する．

定　理 | 4.5.2

$(X, \{\Gamma_i | 1 \leqq i \leqq d\})$ をクラス d のアソシエーションスキームとするとき，以下の等式が成り立つ．

（1）　$p_{ij}^h = p_{ji}^h$

（2）　$n_h p_{ij}^h = n_i p_{hj}^i$

（3）　$\sum_{j=0}^{d} p_{ij}^h = n_i$

（4）　$\sum_{t=0}^{d} p_{li}^t \, p_{tj}^h = \sum_{s=0}^{d} p_{ls}^h \, p_{ij}^s$

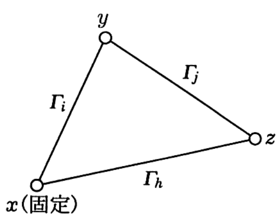
証　明

(1)　定義より明らか．

(2)　X の任意の元 x をとり，それを固定する．そして，集合

$$\{(y, z) \mid y, z \in X,\ x \text{ と } y \text{ は } \Gamma_i \text{ の関係},\ x \text{ と } z \text{ は } \Gamma_h \text{ の関係},\ y \text{ と } z \text{ は } \Gamma_j \text{ の関係}\}$$

の元の個数を 2 通りに求めればよい．



(3)　Γ_h の関係にある X の元 x, y をとり，それらを固定する．このとき，

$$\bigcup_{j=0}^{d} \{z \in X \mid x \text{ と } z \text{ は } \Gamma_i \text{ の関係},\ y \text{ と } z \text{ は } \Gamma_j \text{ の関係}\}$$

$$= \{z \in X \mid x \text{ と } z \text{ は } \Gamma_i \text{ の関係}\}$$

から与式は直ちに得られる．

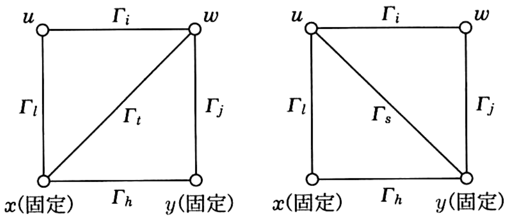
(4)　Γ_h の関係にある X の元 x, y をとり，それらを固定する．このとき，

$$\{(u,w)\mid u,w\in X,\ x \text{ と } u \text{ は } \Gamma_l \text{ の関係},\ u \text{ と } w \text{ は } \Gamma_i \text{ の関係},\ y \text{ と } w \text{ は } \Gamma_j \text{ の関係}\}$$

$$=\bigcup_{t=0}^{d}\{(u,w)\mid u,w\in X,\ x \text{ と } u \text{ は } \Gamma_l \text{ の関係},\ u \text{ と } w \text{ は } \Gamma_i \text{ の関係},\ y \text{ と } w \text{ は } \Gamma_j \text{ の関係},\ x \text{ と } w \text{ は } \Gamma_t \text{ の関係}\}$$

$$=\bigcup_{s=0}^{d}\{(u,w)\mid u,w\in X,\ x \text{ と } u \text{ は } \Gamma_l \text{ の関係},\ u \text{ と } w \text{ は } \Gamma_i \text{ の関係},\ y \text{ と } w \text{ は } \Gamma_j \text{ の関係},\ u \text{ と } y \text{ は } \Gamma_s \text{ の関係}\}$$

から与式は直ちに得られる(下図参照).



さて，クラス d のアソシエーションスキーム $(X,\{\Gamma_i|1\leqq i\leqq d\})$ に対して，

$$n=|X|,\qquad X=\{x_1,x_2,\cdots,x_n\},\qquad A_0=I_n\qquad (n \text{ 次単位行列})$$

とおく．そして，$\Gamma_i\,(1\leqq i\leqq d)$ に関する**隣接行列** A_i を次のように定める．A_i は n 次正方行列で，

$$A_i \text{ の } (s,t) \text{ 成分} =\begin{cases}1 & (\{x_s,x_t\}\in\Gamma_i \text{ のとき})\\ 0 & (\text{その他})\end{cases}.$$

なお，A_0 は便宜上，Γ_0 に関する隣接行列とみなす．このとき，アソシエーションスキームの定義から，

$$A_iA_j=\sum_{h=0}^{d}p_{ij}^{h}A_h$$

がすべての $i,j\in\{0,1,\cdots,d\}$ に対し成り立つことが分かる．したがって，集合

$$S=\{r_0A_0+r_1A_1+\cdots+r_dA_d\mid r_i\in \boldsymbol{R}\}$$

は実数を係数とする n 次正方行列全体からなる環 $M(n,\boldsymbol{R})$ の部分環となる．明らかに，S は $\boldsymbol{R}$ 上の $d+1$ 次元線形空間であり，$\boldsymbol{R}$ の任意の元 r と S の任

意の元 x, y に対して

$$(rx)y = x(ry) = r(xy)$$

が成り立つ．さらにすべての i, j に対して $A_iA_j = A_jA_i$ となるので，S は可換環になる．ここで代数学の専門用語を用いれば，S は $\boldsymbol{R}$ 上の可換多元環となる．本書では，多元環については説明しないが，S を一般にアソシエーションスキーム $(X, \{\Gamma_i | 1 \leqq i \leqq d\})$ に関する**ボーズ-メスナー多元環**という．なお，$A_0, A_1, \cdots, A_d$ は互いに交換可能な実対称行列であるから，ある直交行列 Q があって，$Q^{-1}A_iQ\ (i = 0, 1, \cdots, d)$ は同時に対角行列になることに留意する（[和；6] 参照）．

次に，各 $i\ (i = 0, 1, \cdots, d)$ に対し，(j, h) 成分が p_{ij}^h となる $d+1$ 次正方行列を P_i とおく（$j = 0, 1, \cdots, d$，$h = 0, 1, \cdots, d$）．とくに，P_0 は $d+1$ 次単位行列である．また，$P_0, P_1, \cdots, P_d$ の第1行（$j = 0$ に対応する行）に注目すると，$M(d+1, \boldsymbol{R})$ の元である $P_0, P_1, \cdots, P_d$ は $\boldsymbol{R}$ 上1次独立であることが分かる．一方，定理 4.5.2 を用いることにより，すべての $i, j \in \{0, 1, \cdots, d\}$ に対して

$$P_iP_j = \sum_{h=0}^{d} p_{ij}^h P_h$$

が成り立つことが分かる．そこで，環 $M(d+1, \boldsymbol{R})$ の部分環

$$T = \{r_0P_0 + r_1P_1 + \cdots + r_dP_d \,|\, r_i \in \boldsymbol{R}\}$$

をとると，各 A_i を $P_i\ (i = 0, 1, \cdots, d)$ に対応させる写像を S から T の上への線形空間としての同型写像 φ へ自然に拡張できるだけでなく，$\boldsymbol{R}$ の任意の元 r と S の任意の元 x, y に対して

$$\varphi(rx) = r\varphi(x), \qquad \varphi(xy) = \varphi(x)\varphi(y)$$

も成り立つことになる．（φ は S から T の上への多元環としての同型写像になる．）

行列 $P_0, P_1, \cdots, P_d$ をアソシエーションスキーム $(X, \{\Gamma_i | 1 \leqq i \leqq d\})$ に関する**交叉行列**ということにする．上で述べたことから，各 A_i と P_i の最小多項式は一致する（$i = 0, 1, \cdots, d$）．したがって，それらの相異なる固有値の集合は一致する．普通，A_i の次数 $|X| = n$ に比べて P_i の次数 $d+1$ はかなり小さい

ものであり，A_i の固有値に関する議論は困難であっても，P_i のそれは難しくない場合がある．この点が，アソシエーションスキームの研究が発展している1つの理由であろう．

次の本質的に Biggs による定理の証明は省略するが([洋；2] 参照)，アソシエーションスキームの研究では極めて有力な整数条件である．なお，アソシエーションスキームについての詳しい解説書には，それはより一般化した形で述べられている．

定　理 | 4.5.3

$|X|=n$ であるクラス d のアソシエーションスキーム $(X, \{\Gamma_i \mid 1 \leqq i \leqq d\})$ に関して，$A_i (i=0,1,\cdots,d)$，$P_i (i=0,1,\cdots,d)$ をそれぞれ上記のように定めた隣接行列，交叉行列とする．このとき，θ が P_j の重複度1の固有値とすると，A_j の固有値としての θ の重複度は

$$\frac{n}{(\boldsymbol{u}, \boldsymbol{w})}$$

で与えられる．ただし，$\boldsymbol{u}=(u_0, u_1, \cdots, u_d)$ は $u_0=1$ となる P_j の左固有ベクトル $(\boldsymbol{u}P_j=\theta\boldsymbol{u})$ で，${}^t\boldsymbol{w}={}^t(w_0, w_1, \cdots, w_d)$ は $w_0=1$ となる P_j の右固有ベクトル $(P_j{}^t\boldsymbol{w}=\theta{}^t\boldsymbol{w})$ で，$(\boldsymbol{u}, \boldsymbol{w})$ は $\boldsymbol{u}$ と $\boldsymbol{w}$ の普通の内積である．

以後，シュタイナーシステム $S(t,k,v)$ の場合について考える．$(\Omega, \boldsymbol{B})$ をシュタイナーシステム $S(t,k,v)$ とし，B, B' をそのブロックとするとき，$|B \cap B'|$ を B と B' の**交叉数**ということにする．この場合，交叉数は $0,1,\cdots,t-1,k$ のどれかであるが，B と交叉数が i となるブロックの個数を $x_i(B)$ で表す．

定　理 | 4.5.4

$(\Omega, \boldsymbol{B})$ をシュタイナーシステム $S(t,k,v)$ とし，B を任意に固定した1つのブロックとすると，$i=0,1,\cdots,t-1$ に対し

$$x_i(B)=\sum_{j=i}^{t-1}\binom{j}{i}(\lambda_j-1)\binom{k}{j}(-1)^{i+j}$$

である．とくに，$x_i(B)$ は B のとり方によらない数である．

証　明

$i=0,1,\cdots,t-1$ に対し，集合

$\{(B',\{\alpha_1,\alpha_2,\cdots,\alpha_i\})\,|\,B\neq B'\in \boldsymbol{B},\ \alpha_1,\cdots,\alpha_i$ は相異なる $B\cap B'$ の元$\}$

の元の個数を2通りに計算すると，以下の t 個の式を得る．

$$x_0(B)+x_1(B)+x_2(B)+\cdots\cdots\cdots+x_{t-1}(B)=\lambda_0-1$$

$$x_1(B)+2x_2(B)+\cdots\cdots\cdots+(t-1)x_{t-1}(B)=(\lambda_1-1)\binom{k}{1}$$

$$\cdots\cdots\cdots$$

$$x_{t-2}(B)+\binom{t-1}{t-2}x_{t-1}(B)=(\lambda_{t-2}-1)\binom{k}{t-2}$$

$$x_{t-1}(B)=(\lambda_{t-1}-1)\binom{k}{t-1}$$

よって，A を (i,j) 成分が $\binom{j}{i}$ である t 次正方行列とすると $(i=0,1,\cdots,t-1,\ j=0,1,\cdots,t-1)$，

$$A\begin{pmatrix}x_0(B)\\x_1(B)\\\vdots\\x_{t-2}(B)\\x_{t-1}(B)\end{pmatrix}=\begin{pmatrix}\lambda_0-1\\(\lambda_1-1)\binom{k}{1}\\\vdots\\(\lambda_{t-2}-1)\binom{k}{t-2}\\(\lambda_{t-1}-1)\binom{k}{t-1}\end{pmatrix}$$

が成り立つ．ここで A は正則行列で，その逆行列は (i,j) 成分が $\binom{j}{i}(-1)^{i+j}$ となる行列であることが以下のようにして分かるので，結論を得る．

二項定理より，変数 x に対して

$$(1+x)^j = \sum_{h=0}^{j} \binom{j}{h} x^h$$

が成り立つ．両辺を x で i 回 $(i \leqq j)$ 微分して，両辺を $i!$ で割り，そして $x = -1$ を代入すると，

$$\sum_{h=i}^{j} \binom{j}{h} \binom{h}{i} (-1)^{h+i} = \delta_{ij}$$

を得る(δ_{ij} はクロネッカーのデルタ)．

定理4.5.4より，シュタイナーシステム $S(t, k, v)$ はブロックどうしの交叉数の関係に関してアソシエーションスキームの定義の(1)をみたすことが分かる．もちろん，アソシエーションスキームの定義の(2)までをみたすシュタイナーシステムは稀であるが，$t = 2$ のシュタイナーシステム $S(2, k, v)$ は，ブロックどうしの交叉数の関係に関してアソシエーションスキームになることが上記の結果を用いて簡単に確かめられる．

一方，その説明は省略するが，$(t, k, v) = (3, 4, 8)$，$(4, 5, 11)$，$(5, 6, 12)$，$(3, 6, 22)$，$(4, 7, 23)$ または $(5, 8, 24)$ のときは，置換群的な考察により次のことがいえる：シュタイナーシステム $S(t, k, v)$ のブロック B_1，B_2，B_3，B_4 が

$$|B_1 \cap B_2| = |B_3 \cap B_4|$$

をみたせば，

$$(B_1)g = B_3, \qquad (B_2)g = B_4$$

となる $S(t, k, v)$ の自己同型写像 g が存在する．なお，$S(3, 4, 8)$ は同型を除いてただ1つのみ存在し，その自己同型群は点集合上3重可移に作用する位数1344の群である([洋；3] 参照)．

したがって，$S(3, 4, 8)$ と5つのウィットシステムはどれも，ブロックどうしの交叉数の関係に関してアソシエーションスキームになることが分かる．次の定理は，それら6個のシュタイナーシステムを，群の作用を一切仮定しないでアソシエーションスキームの立場から特徴付けたものである．

定 理 | 4.5.5 ……………………………………………Yoshizawa[論；38, 40]

(1) $t \geqq 2$ のシュタイナーシステム $S(t, t+1, v)$ が，ブロックどうしの交叉数の関係に関してアソシエーションスキームになるための必要十分条件は，$t=2$ であるか $(t, t+1, v) = (3, 4, 8)$，$(4, 5, 11)$ または $(5, 6, 12)$ をみたすことである．

(2) $t \geqq 2$ のシュタイナーシステム $S(t, t+3, v)$ が，ブロックどうしの交叉数の関係に関してアソシエーションスキームになるための必要十分条件は，$t=2$ であるか $(t, t+3, v) = (3, 6, 22)$，$(4, 7, 23)$ または $(5, 8, 24)$ をみたすことである．

5 章

群とグラフ

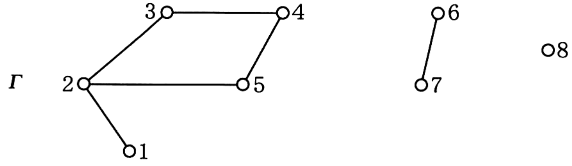
5.1 グラフ

グラフ理論は，位相数学的なオイラーの一筆書き問題を起源とし，化学の分子式，電子工学の回路などとも関連して発展してきたことは一般によく知られている．一方で，群との関係から発展してきた側面もあり，本書では主にその方面について述べる．そして本節では，グラフの基礎的事項について説明しよう．

空でない集合 V と $V^{(2)}$ の部分集合 E との組 $\Gamma = (V, E)$ を**(無向)グラフ**という．V を**頂点集合**，V の元を**頂点**といい，E を**辺集合**，E の元を**辺**という．また，$|V|$, $|E|$ をそれぞれ Γ の**位数**，**サイズ**という．Γ の位数が有限か無限であるかにしたがって，Γ を**有限グラフ**あるいは**無限グラフ**という．一般に次の例のように，頂点を小マルで，辺を頂点どうしを結ぶ線で図示することが多い．

例 5.1.1

$\Gamma = (V, E)$, $V = \{1, 2, 3, 4, 5, 6, 7, 8\}$, $E = \{\{1, 2\}, \{2, 3\}, \{2, 5\}, \{3, 4\}, \{4, 5\}, \{6, 7\}\}$.



グラフにおいても，群やデザインと同様に同型の概念が次のように定義される．2 つのグラフ $\Gamma_1 = (V_1, E_1)$，$\Gamma_2 = (V_2, E_2)$ に対し，V_1 から V_2 への全単射

φ があって，

$$\{u, v\} \in E_1 \Longleftrightarrow \{(u)\varphi, (v)\varphi\} \in E_2$$

が成り立つとき，φ を Γ_1 から Γ_2 の上への**同型写像**であるといい，Γ_1 と Γ_2 は**同型**であるという．

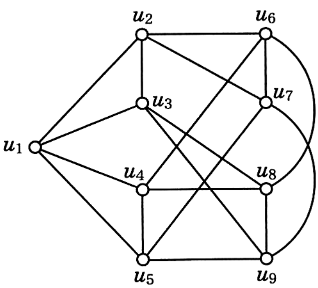
グラフ $\Gamma = (V, E)$ に対し，Γ から Γ の上への同型写像全体からなる集合は写像の合成に関して群になるが，それを Γ の**自己同型群**といい $\mathrm{Aut}(\Gamma)$ で表す．また，$\mathrm{Aut}(\Gamma)$ の各元を Γ の**自己同型写像**という．$\mathrm{Aut}(\Gamma)$ は V 上の置換群であり，それはデザインの場合と比べて扱いやすい面が多い．

例 | 5.1.2

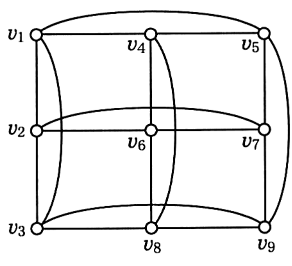
次の 2 つのグラフは同型である．実際，

$$(u_i)\varphi = v_i \qquad (i = 1, 2, \cdots, 9)$$

によって定められる写像 φ は Γ_1 から Γ_2 の上への同型写像である．



Γ_1



Γ_2

なお，集合 V と直積集合 $V \times V$ の部分集合 A との組 $\Gamma = (V, A)$ は**有向グラフ**といい，電子工学ばかりでなく経営数学等の応用面でも重要であるが（[和；13] 参照），本書では扱わないことにする．

グラフ $\Gamma = (V, E)$ において，$e = \{u, v\} \in E$ のとき，u と v は**隣接**しているといい，u は e に**接続**しているという．Γ の頂点 v に対し

$$N_\Gamma(v) = \{u \in V \mid \{u, v\} \in E\}$$

とおき，それを Γ における v の**近傍**という．なお，$N_\Gamma(v)$ は単に $N(v)$ で表すこともある．$|N_\Gamma(v)|$ を Γ における v の**次数**といい，$\deg_\Gamma(v)$ あるいは単に

$\deg(v)$ で表す．たとえば，例 5.1.1 において

$$N(2) = \{1, 3, 5\}, \qquad \deg(2) = 3$$

である．

定 理 | 5.1.3

有限グラフ $\Gamma = (V, E)$ において，

$$\sum_{v \in V} \deg(v) = 2|E|$$

が成り立つ．とくに，奇数次数の頂点の個数は偶数個である．

証 明

集合

$$\{(v, e) | v \in V,\ e \in E,\ v \text{ は } e \text{ に接続}\}$$

の元の個数を 2 通りに計算することによって得られる．

グラフ $\Gamma' = (V', E')$ がグラフ $\Gamma = (V, E)$ の部分グラフであるとは，

$$V' \subseteqq V, \qquad E' \subseteqq E$$

のときにいう．

たとえば例 5.1.1 において，

$$V' = \{1, 2, 3, 4, 5\}, \qquad E' = \{\{1, 2\}, \{2, 3\}, \{2, 5\}\}$$

とすると，$\Gamma' = (V', E')$ は $\Gamma = (V, E)$ の部分グラフである．

グラフ $\Gamma = (V, E)$ において，頂点の列

$$P = (v_0, v_1, \cdots, v_s)$$

は，$\{v_{i-1}, v_i\} \in E\,(i = 1, 2, \cdots, s)$ のとき**長さ** s の**道**といい，v_0 と v_s をそれぞれ P の**始点**，**終点**という．とくに $v_0 = v_s$ で，P を構成する頂点のうちで一致するのがそれだけのとき，P を**長さ** s の**サイクル**という．

たとえば例 5.1.1 において，$(2, 3, 4, 5, 2)$ は長さ 4 のサイクルである．

グラフ $\Gamma = (V, E)$ において，u と v が Γ の頂点であるとき，u と v の距離 $d(u, v)$ を次のように定める．

$$d(u,v)=\begin{cases}0 & (u=v\text{ のとき})\\ \infty & (u\text{ と }v\text{ を結ぶ道がないとき})\\ u\text{ と }v\text{ を結ぶ長さ最小の道の長さ} & \\ \qquad (u\text{ と }v\text{ を結ぶ道があるとき}) & \end{cases}$$

もし，Γ の任意の 2 頂点間の距離が有限であるとき，Γ は**連結**であるという．そうでないとき，Γ は**非連結**であるという．また，グラフ Γ の連結な部分グラフ $\Gamma'=(V',E')$ に対し，$V'\subsetneq X$ あるいは $E'\subsetneq Y$ となる Γ の連結な部分グラフ $\Delta=(X,Y)$ がないとき，Γ' を Γ の**連結成分**という．

たとえば，例 5.1.1 のグラフ Γ は非連結で，それは 3 つの連結成分から成り立っている．

次の例は，**ラムゼー現象**とよばれるものの一つである．

例 | 5.1.4

6 頂点からなるグラフ $\Gamma=(V,E)$ は，次の(1)または(2)の異なる 3 頂点 v_1, v_2, v_3 を必ずもつ．

（1） $\{v_1,v_2\}\notin E$,　 $\{v_1,v_3\}\notin E$,　 $\{v_2,v_3\}\notin E$.

（2） $\{v_1,v_2\}\in E$,　 $\{v_1,v_3\}\in E$,　 $\{v_2,v_3\}\in E$.

なぜならば，Γ が 3 つ以上の連結成分をもつときは，各々の連結成分から 1 つずつ頂点をとることによって(1)の成立が分かる．

また，Γ がちょうど 2 つの連結成分 $\Gamma_1=(V_1,E_1)$，$\Gamma_2=(V_2,E_2)$ をもつグラフであるときは，一般性を失わないで $|V_1|\geqq 3$ としてよい．x_1, x_2, x_3 を Γ_1 の異なる 3 頂点とし，y を Γ_2 の頂点とすると，$\{y,x_i\}\notin E\,(i=1,2,3)$ であるので，もしある $i\neq j$ に対して $\{x_i,x_j\}\notin E$ ならば，(1)の成立が分かる．もし $\{x_1,x_2\}$，$\{x_1,x_3\}$，$\{x_2,x_3\}\in E$ ならば，それは(2)の成立を意味している．

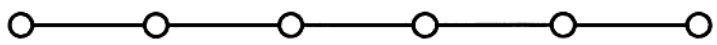
そして，Γ が連結グラフであるときは，$\deg(x)\geqq 3$ となる頂点 x がある場合とない場合とに分けて考える．そのような x があるときは，

$$\{x,y_i\}\in E \qquad (i=1,2,3)$$

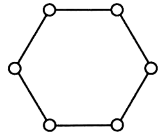
となる 3 頂点 y_1, y_2, y_3 をもつが，ある $i\neq j$ に対して $\{y_i,y_j\}\in E$ ならば，(2)の成立が分かる．もし $\{y_1,y_2\}\notin E$，$\{y_1,y_3\}\notin E$，$\{y_2,y_3\}\notin E$ ならば，これは(1)

の成立を意味している．

最後に，Γ が連結で，すべての頂点の次数が 1 または 2 ならば，Γ は次の Δ_1 か Δ_2 と同型になるので，(1)の成立が分かる（下図参照）．



Δ_1



Δ_2

グラフ $\Gamma = (V, E)$ において，

$$\Gamma \text{ の}\textbf{直径} = \begin{cases} \infty & (\{d(u,v) \mid u, v \in V\} \text{ が有界でないとき}) \\ \max\{d(u,v) \mid u, v \in V\} & \\ & (\{d(u,v) \mid u, v \in V\} \text{ が有界のとき}) \end{cases}$$

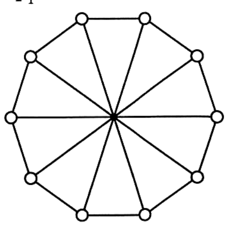
$$\Gamma \text{ の}\textbf{内周長} = \begin{cases} \infty & (\Gamma \text{ にサイクルがないとき}) \\ \min\{s \mid \Gamma \text{ は長さ } s \text{ のサイクルをもつ}\} & \\ & (\Gamma \text{ にサイクルがあるとき}) \end{cases}$$

と定める．2 つのグラフ Γ_1 と Γ_2 が同型ならば，それらの直径や内周長は等しい．

例 | 5.1.5

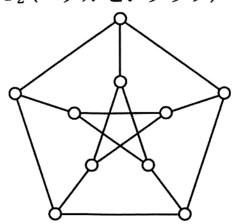
次のグラフ Γ_1, Γ_2 はともに 10 頂点からなる連結グラフで，各頂点の次数は 3 である．しかしながら，それらの直径と内周長は異なる．

Γ_1



Γ_1 の直径 $= 3$
Γ_1 の内周長 $= 4$

Γ_2（ペテルセングラフ）

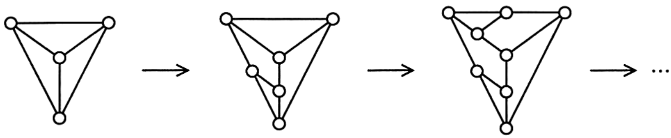


Γ_2 の直径 $= 2$
Γ_2 の内周長 $= 5$

すべての頂点の次数が等しいグラフを**正則グラフ**という．そして各頂点の次数が k であるとき，それを k-**正則**グラフともいう．例 5.1.5 のグラフは，どちらも 3-正則グラフである．

例 | 5.1.6

4 以上の任意の偶数 n に対し，n 頂点からなる連結な 3-正則グラフは存在する．実際，次のように次々と新しい頂点と辺を加えたグラフを考えれば分かる．



例 5.1.6 のグラフのように，平面上に図示したものが，どの 2 つの辺もそれらを構成する頂点以外では交わっていないとき，それを**平面グラフ**という．また，平面グラフと同型なグラフは**平面的グラフ**という．平面的グラフに関しては，位相数学的に特徴付けたクラトウスキーの定理が有名である([和；2] 参照)．

ここで，特定の記法をもつグラフを例として紹介しておく．

例 | 5.1.7

(ア)　道の定義のところで述べた長さ s のサイクルを，それ自身グラフと考えて C_s で表す．$s \geqq 3$ のとき，C_s の頂点集合 V と辺集合 E を

$$V = \{1, 2, \cdots, s\}, \qquad E = \{\{1, 2\}, \{2, 3\}, \cdots, \{s-1, s\}, \{s, 1\}\}$$

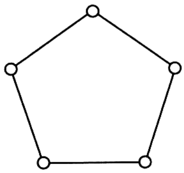
によって表せば，

$$\mathrm{Aut}(C_s) = \langle a, b\rangle,$$

$$a = \begin{pmatrix} 1 & 2 & 3 & \cdots & s-1 & s \\ 2 & 3 & 4 & \cdots & s & 1 \end{pmatrix}, \qquad b = \begin{pmatrix} 1 & 2 & 3 & \cdots & s-1 & s \\ 1 & s & s-1 & \cdots & 3 & 2 \end{pmatrix},$$

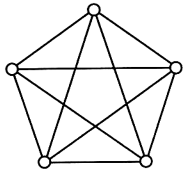
$$|a| = s, \qquad |b| = 2, \qquad b^{-1}ab = a^{-1}, \qquad |\langle a, b\rangle| = 2s$$

である．なお置換群に限らず，このような群を一般に位数 $2s$ の**2 面体群**という．



C_5

（イ） 自然数 n に対し，n 個の頂点からなるグラフ $\Gamma=(V,E)$ で，辺集合 E が $V^{(2)}$ と一致するものを n 頂点からなる**完全グラフ**といい，K_n で表す．明らかに，$\mathrm{Aut}(K_n)$ は n 次対称群 S_n である．



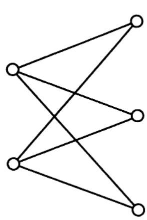
K_5

（ウ） 自然数 m,n に対し，次のような $m+n$ 個の頂点からなるグラフ $\Gamma=(V,E)$ を**完全 2 部グラフ** $K_{m,n}$ という．

$$V=\{u_1,u_2,\cdots,u_m,v_1,v_2,\cdots,v_n\},$$

$$E=\{\{u_i,v_j\}\mid 1\leqq i\leqq m,\ 1\leqq j\leqq n\}.$$

$m\neq n$ のとき，$\mathrm{Aut}(K_{m,n})$ は m 次対称群 S_m と n 次対称群 S_n の直積 $S_m\times S_n$ となる．また $m=n$ のとき，$\mathrm{Aut}(K_{m,n})$ は m 次対称群 S_m と 2 次対称群 S_2 のレス積となる（レス積については 4.5 節を参照）．



$K_{2,3}$

（ウ）の完全 2 部グラフを一般化した 2 部グラフの概念は重要であり，その定義を述べておく．グラフ $\Gamma=(V,E)$ が **2 部グラフ**であるとは，V が部分集合 V_1 と V_2 の直和として表され，任意の $\{u,v\}\in E$ に対し，

$$u \in V_1, \quad v \in V_2$$

または

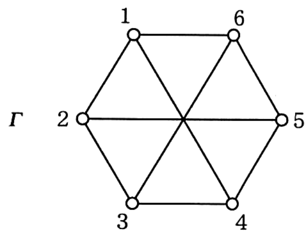
$$v \in V_1, \quad u \in V_2$$

が成り立つことである．

5.2 グラフの自己同型群として表現する群

本節では，グラフに作用する群を考えるときに重要なケイリーグラフについて述べることを一つの目標とする．前節でグラフの自己同型群を定義したが，最初に次の例のグラフ Γ を考えてみよう．

例 5.2.1



$\mathrm{Aut}(\Gamma)$ は巡回置換 $(1\ \ 2\ \ 3\ \ 4\ \ 5\ \ 6)$ を含むので，$\mathrm{Aut}(\Gamma)$ は V 上可移に作用する．そして，$\mathrm{Aut}(\Gamma)$ における頂点 1 の固定部分群 $\mathrm{Aut}(\Gamma)_1$ を考えると，1 から距離 1 の集合 $\{2,4,6\}$ と 1 から距離 2 の集合 $\{3,5\}$ の上に作用しなくてはならない．ところが，

$$\mathrm{Aut}(\Gamma) \ni (2\ \ 4\ \ 6),\ (2\ \ 4),\ (3\ \ 5)$$

なので，$\mathrm{Aut}(\Gamma)_1$ は $\{2,4,6\}$ 上の 3 次対称群と $\{3,5\}$ 上の 2 次対称群の直積となる．したがって，定理 1.3.2 より

$$|\mathrm{Aut}(\Gamma)| = 6 \times |\mathrm{Aut}(\Gamma)_1| = 72.$$

上記のグラフのように，自己同型群が頂点集合上可移に作用しているグラフを**頂点可移グラフ**という．その自己同型群の位数を求める場合は，上のように 1 つの頂点の固定部分群の位数を求める方法がよい．

グラフ $\Gamma(V, E)$ の自己同型群 $\mathrm{Aut}(\Gamma)$ が E 上可移に作用するとき，Γ を**辺可移グラフ**という．$m \neq n$ である完全2部グラフは辺可移グラフであるが頂点可移グラフではない．また，辺可移な正則グラフで頂点可移でないグラフも存在する([論；6] 参照)．

定　理 | 5.2.2

$\Gamma = (V, E)$ を，辺可移であるが頂点可移ではない連結グラフとする．このとき，Γ は2部グラフである．

証　明

$\{u, v\}$ を Γ の辺とし，

$$V_1 = \{(u)\varphi \mid \varphi \in \mathrm{Aut}(\Gamma)\}, \qquad V_2 = \{(v)\varphi \mid \varphi \in \mathrm{Aut}(\Gamma)\}$$

とおく．Γ は連結で辺可移なので，Γ の任意の頂点 x は V_1 か V_2 に属することになる．もし

$$V_1 \cap V_2 \neq \emptyset$$

とすると，Γ は頂点可移となって，仮定に反する．また，ある辺 $\{u', v'\}$ に対し，$u', v' \in V_1$ または $u', v' \in V_2$ が成り立つとすると，$V_1 \cap V_2 \neq \emptyset$ が導かれて矛盾である．

次に，ケイリーグラフを定義しよう．G を群とし，S を次の条件をみたす G の部分集合とする：$S \not\ni 1$ で，

$$x \in S \Longrightarrow x^{-1} \in S$$

このとき，**ケイリーグラフ** $\Gamma = \Gamma(G\,;S) = (V, E)$ とは，次のように定めるグラフのことである．

$$V = G, \qquad E = \{\{g, h\} \mid gh^{-1} \in S\}.$$

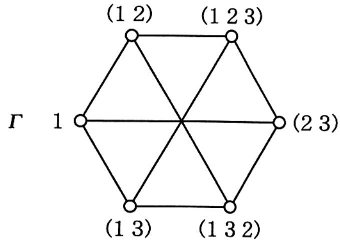
実際，$gh^{-1} \in S$ のとき，

$$hg^{-1} = (gh^{-1})^{-1} \in S$$

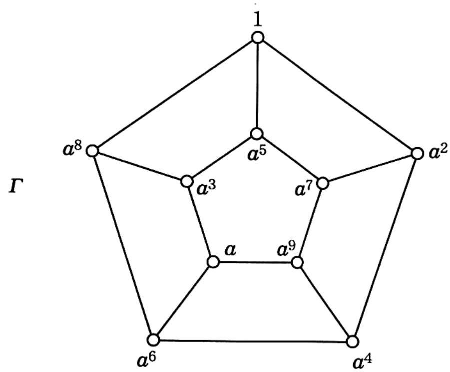
となるので，上の定義に問題はない．

例 | 5.2.3

（ア） G を $\{1, 2, 3\}$ 上の 3 次対称群，$S = \{(1 \quad 2), (1 \quad 3), (2 \quad 3)\}$ とおくと，ケイリーグラフ $\Gamma = \Gamma(G\,;S)$ は例 5.2.1 のグラフになる．



（イ） G を元 a で生成される位数 10 の巡回群とし，$S = \{a^2, a^5, a^8\}$ とおくと，ケイリーグラフ $\Gamma = \Gamma(G\,;S)$ は次のグラフになる．



ちなみに，

$$\mathrm{Aut}(\Gamma) \ni (1, a^2, a^4, a^6, a^8)(a^5, a^7, a^9, a, a^3),$$
$$(1 \quad a^5)(a^8 \quad a^3)(a^6 \quad a)(a^4 \quad a^9)(a^2 \quad a^7)$$

なので，$\mathrm{Aut}(\Gamma)$ は頂点集合 G 上に可移に作用している．

さらに，$\mathrm{Aut}(\Gamma)$ における頂点 1 の固定部分群は

$$\mathrm{Aut}(\Gamma)_1 = \{1, (a^8 \quad a^2)(a^3 \quad a^7)(a^6 \quad a^4)(a \quad a^9)\}$$

となることがやさしく分かる．したがって，$|\mathrm{Aut}(\Gamma)| = 20$ である．

定　理｜5.2.4

ケイリーグラフ $\Gamma = \Gamma(G\,;S) = (V, E)$ について次のことが成り立つ．

（1）　$G = \langle S \rangle$ ならば Γ は連結である．

（2）　Γ は頂点可移グラフで，$\mathrm{Aut}(\Gamma)$ は V 上正則に作用する G と同型な部分群 $\bar{G}$ をもつ．

（3）　群 G の自己同型写像 σ が $(S)\sigma = S$ をみたすならば，σ を V 上の置換とみなすと，σ は頂点 1 を固定する Γ の自己同型写像になる．

証　明

（1）　G の任意の元 g に対し，

$$g = g_1 g_2 \cdots g_s$$

となる S の元 $g_1, g_2, \cdots, g_s$ がある．このとき，頂点列

$$(1,\ g_s,\ g_{s-1}g_s,\ g_{s-2}g_{s-1}g_s,\ \cdots,\ g_1g_2\cdots g_{s-1}g_s)$$

は Γ における道になる．よって，Γ の任意の頂点は頂点 1 と道によって結ばれている．

（2）　G の各元 g に対し，V 上の置換 $\bar{g}$ を次のように定める．V のすべての元 h に対し，

$$(h)\bar{g} = hg.$$

このとき，$\bar{g} \in \mathrm{Aut}(\Gamma)$ となる．実際，

$$\begin{aligned}\{u, v\} \in E &\Longleftrightarrow uv^{-1} \in S \\ &\Longleftrightarrow (ug)(vg)^{-1} \in S \\ &\Longleftrightarrow \{(u)\bar{g}, (v)\bar{g}\} \in E.\end{aligned}$$

いま，$\bar{G} = \{\bar{g} \mid g \in G\}$ とおけば，$\bar{G}$ は $\mathrm{Aut}(\Gamma)$ の部分群で，V 上正則に作用する．

（3）　$1^\sigma = 1$ は明らか．また，

$$\begin{aligned}\{u, v\} \in E &\Longleftrightarrow uv^{-1} \in S \\ &\Longleftrightarrow (uv^{-1})\sigma \in S \\ &\Longleftrightarrow (u^\sigma)(v^\sigma)^{-1} \in S\end{aligned}$$

$$\Longleftrightarrow \{u^{\sigma}, v^{\sigma}\} \in E$$

なので，$\sigma \in \mathrm{Aut}(\Gamma)$ である．

ここで，定理 5.2.4 における(1)の仮定をケイリーグラフの定義に加えている書もあることを注意する．

定理 | 5.2.5

グラフ $\Gamma = (V, E)$ に対し，$\mathrm{Aut}(\Gamma)$ が V 上正則に作用する部分群をもつための必要十分条件は，Γ があるケイリーグラフ $\Delta = \Delta(H\,;S)$ と同型になることである．

証明

定理 5.2.4(2)により十分性は明らかなので，必要性を示せばよい．いま，$\mathrm{Aut}(\Gamma)$ が V 上正則に作用する部分群 H をもつとする．V の一つの元 v_0 を固定すると，V の任意の元 v に対し，$(v_0)h = v$ となる H の元 h はただ一つ存在する．したがって，その対応により V から H への全単射 φ が定まる．ここで，

$$S = \{h \in H \mid (v_0)h \in N(v_0) \quad (v_0 \text{ の近傍})\}$$

とおくと，ケイリーグラフ $\Delta = \Delta(H\,;S)$ が定義される．実際，$S \not\ni 1$ は明らかである．また，v_0 と $(v_0)h$ が隣接ならば $(v_0)h^{-1}$ と v_0 は隣接である．すなわち，$S \ni h$ ならば $S \ni h^{-1}$ である．

以上のもとで，φ が Γ から Δ の上への同型写像になることが次のようにして分かる．u, v を Γ の頂点とすると，

$$(v_0)h_1 = u, \quad (v_0)h_2 = v$$

となる H の元 $h_1 = (u)\varphi$，$h_2 = (v)\varphi$ がある．そして，

$$\begin{aligned} & u \text{ と } v \text{ は } \Gamma \text{ において隣接} \\ \Longleftrightarrow\ & (v_0)h_1 \text{ と } (v_0)h_2 \text{ は } \Gamma \text{ において隣接} \\ \Longleftrightarrow\ & v_0 \text{ と } (v_0)h_2h_1^{-1} \text{ は } \Gamma \text{ において隣接} \end{aligned}$$

$\Longleftrightarrow h_2h_1^{-1} \in S$

$\Longleftrightarrow h_2$ と h_1 は $\varDelta$ において隣接

一般に，群 G が**グラフ正則表現**をもつとは，次のグラフ $\Gamma = (V, E)$ が存在することである：$\mathrm{Aut}(\Gamma)$ は群として G と同型で，置換群として V 上正則に作用している．定理 5.2.5 を踏まえれば，この定義は必然的なものであろう．

ケイリーグラフはグラフ正則表現のためだけではなく，様々な形で研究が発展している．しかしながらグラフ正則表現をもつ有限群の研究は，ケイリーグラフにとって一つの目標であったことは言うまでもない．それに関しては，次の三つの定理によって分類が完成している．定理 5.2.7 で述べる "10 個の群" が載っている文献は，［論；13］が分かりやすい．

なお，一般に群 G が**可解**であるとは，次の条件をみたすことである：

$$G = H_0 \trianglerighteq_{\neq} H_1 \trianglerighteq_{\neq} H_2 \trianglerighteq_{\neq} \cdots \trianglerighteq_{\neq} H_r = 1$$

のように，各 H_{i+1} が H_i の真部分群かつ正規部分群となる G の部分群の有限列があって，すべての H_i/H_{i+1} が可換群である $(i = 0, 1, \cdots, r-1)$．

定理 | 5.2.6 ……………………………………………………Imrich［論；18］

有限可換群 G がグラフ正則表現をもつための必要十分条件は，G が位数 2^s $(s \neq 2, 3, 4)$ の基本可換群であることである．

定理 | 5.2.7 ……………………………………………………Hetzel［論；16］

非可換な有限可解群は，10 個の例外の群を除きすべてグラフ正則表現をもつ．

定理 | 5.2.8 ……………………………………………………Godsil［論；13］

非可解な有限群はすべてグラフ正則表現をもつ．

ところで，定理 5.2.8 の本質的な部分は次の定理である．

定理 | 5.2.9 ……………………………………………………Godsil [論；14]

有限群 G は，G のすべての位数 2 の元からなる部分集合によって生成される群とする．もし $|G| > 18$ ならば，G はグラフ正則表現をもつ．

群をグラフの自己同型群として表現する問題として，次の定理 5.2.10 は一つの出発点であった．定理 5.2.11 は，その自然な延長にあるものである．

定理 | 5.2.10 ……………………………………………………Frucht [論；12]

任意の有限群 G に対し，群として $\mathrm{Aut}(\Gamma) \cong G$ となる連結な3-正則グラフが存在する．

定理 | 5.2.11 ……………………………………………………Yoshizawa [論；39]

G を任意の有限群とし，t を任意の自然数とする．このとき，任意の整数 $n \geqq \max\{|G|, 3\}$ に対し，以下の条件をみたす連結な n-正則グラフ $\Gamma = (V, E)$ は無限個存在する：群として $\mathrm{Aut}(\Gamma) \cong G$ で，Γ には $\mathrm{Aut}(\Gamma) = \mathrm{Aut}(\Gamma)_{\alpha_1\alpha_2\cdots\alpha_t}$ となる t 個の頂点 $\alpha_1, \alpha_2, \cdots, \alpha_t$ があって，$\mathrm{Aut}(\Gamma)$ は $V - I(\mathrm{Aut}(\Gamma))$ 上半正則に作用している．

なお上の定理で，n が $\max\{|G|, 3\}$ 以上である条件は落とすことができない．

5.3 グラフの固有値

本節では，対象とするグラフは有限グラフに限定して考えるものとする．線形代数学の固有値を本質的に用いたグラフの研究は古くから行われており，数多くの興味ある結果が得られている（[洋；11] 参照）．それは群との関係，あるいはアソシエーションスキームの構造をもつグラフの研究へと発展している（[洋；2, 6, 7] 参照）．前者に関しては本節で，後者に関しては 5.4 節で扱うことにする．

グラフ $\Gamma = (V, E)$ の頂点集合 V を $\{v_1, v_2, \cdots, v_n\}$ とするとき，Γ の隣接

行列 $A=A(\Gamma)$ は次のように定める n 次行列である.

$$A \text{ の } (i,j) \text{ 成分} = \begin{cases} 1 & (v_i \text{ と } v_j \text{ は隣接}) \\ 0 & (v_i \text{ と } v_j \text{ は隣接でない}) \end{cases}$$

また, V 上の置換 π に対する**置換行列** P_π は次のように定める n 次行列である.

$$P_\pi \text{ の } (i,j) \text{ 成分} = \begin{cases} 1 & (v_j = (v_i)\pi \text{ のとき}) \\ 0 & (v_j \neq (v_i)\pi \text{ のとき}) \end{cases}$$

V 上の置換行列全体は行列の積に関して群をなし, それは n 次対称群 S_n と同型になることがやさしく分かる. また, P_π の転置行列が P_π の逆行列であり, 任意の n 次正方行列 X の右(左)から P_π をかけると X の列(行)の置換を引き起こし, $P_\pi^{-1}AP_\pi$ は Γ の頂点 $v_1, v_2, \cdots, v_n$ の名称だけを取り替えたグラフの隣接行列になっている. 逆に, $v_1, v_2, \cdots, v_n$ の名称だけを取り替えたグラフの隣接行列は, そのような形で表される. ここで, A と $P_\pi^{-1}AP_\pi$ の固有多項式や最小多項式は, それぞれ等しいことに留意する.

グラフ Γ の隣接行列 A は実対称行列であるから, 直交行列によって対角化され, A の固有値はすべて実数である. そして, A の各固有値 λ の重複度は, λ に対する固有空間の次元と等しい. グラフ Γ の**固有値**, **固有ベクトル**, **固有多項式**, **最小多項式**とは, それぞれ隣接行列 A のそれらとする. また, Γ の相異なる固有値全体を

$$\lambda_1 > \lambda_2 > \cdots > \lambda_s$$

とし, 各 λ_i の重複度を $m(\lambda_i)$ とするとき, Γ の**スペクトラム** $\mathrm{Spec}\,\Gamma$ とは 2 行 s 列行列

$$\begin{pmatrix} \lambda_1 & \lambda_2 & \cdots & \lambda_s \\ m(\lambda_1) & m(\lambda_2) & & m(\lambda_s) \end{pmatrix}$$

のことである. ここで, Γ の最小多項式 $\varphi_\Gamma(x)$ は

$$\varphi_\Gamma(x) = (x-\lambda_1)(x-\lambda_2)\cdots(x-\lambda_s)$$

と表される. 一方, もし Γ が連結で直径が d とすると, $I, A, A^2, \cdots, A^d$ は $\boldsymbol{R}$ 上 1 次独立である. 実際, 頂点 v_i と v_j の距離が h $(1 \leqq h \leqq d)$ とすると, A^h の (i,j) 成分は v_i と v_j を結ぶ道の本数ゆえ 0 ではなく, $I, A, A^2, \cdots, A^{h-1}$ の

(i,j) 成分は0である．

以上をまとめると，次の定理のようになる．

定　理｜5.3.1

n 項点からなる連結グラフ Γ の直径が d とすると，Γ の最小多項式 $\varphi_\Gamma(x)$ の次数 s は $d+1$ 以上 n 以下で，Γ の相異なる固有値の個数は s である．

例｜5.3.2

（ア）　完全グラフ K_n の隣接行列 A は，対角成分だけが0で，その他の成分はすべて1の n 次行列である．よって，

$$\det(xI-A)=\begin{vmatrix} x & -1 & \cdots & \cdots & -1 \\ -1 & x & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & -1 \\ -1 & \cdots & \cdots & -1 & x \end{vmatrix}$$

$$=(x-n+1)\begin{vmatrix} 1 & \cdots & \cdots & \cdots & 1 \\ -1 & x & -1 & \cdots & -1 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & -1 \\ -1 & \cdots & \cdots & -1 & x \end{vmatrix}$$

$$=(x-n+1)\begin{vmatrix} 1 & 1 & \cdots & & 1 \\ & x+1 & & \cdots & \\ & & \ddots & \ddots & O \\ & & & & \\ O & & & & x+1 \end{vmatrix}$$

$$=(x-n+1)(x+1)^{n-1}$$

$$\operatorname{Spec} K_n=\begin{pmatrix} n-1 & -1 \\ 1 & n-1 \end{pmatrix}.$$

（イ）　完全2部グラフ $K_{3,3}$ の隣接行列 A は，

$$\begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \end{pmatrix}$$

としてよい．よって，

$$\det(xI-A) = \begin{vmatrix} x & 0 & 0 & -1 & -1 & -1 \\ 0 & x & 0 & -1 & -1 & -1 \\ 0 & 0 & x & -1 & -1 & -1 \\ -1 & -1 & -1 & x & 0 & 0 \\ -1 & -1 & -1 & 0 & x & 0 \\ -1 & -1 & -1 & 0 & 0 & x \end{vmatrix}$$

$$= (x-3)\begin{vmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & x & 0 & -1 & -1 & -1 \\ 0 & 0 & x & -1 & -1 & -1 \\ -1 & -1 & -1 & x & 0 & 0 \\ -1 & -1 & -1 & 0 & x & 0 \\ -1 & -1 & -1 & 0 & 0 & x \end{vmatrix}$$

$$= (x-3)\begin{vmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & x & 0 & -1 & -1 & -1 \\ 0 & 0 & x & -1 & -1 & -1 \\ -1 & 0 & 0 & x & 0 & 0 \\ -1 & 0 & 0 & 0 & x & 0 \\ -1 & 0 & 0 & 0 & 0 & x \end{vmatrix}$$

$$= (x-3)\,x^2\begin{vmatrix} 1 & 1 & 1 & 1 \\ -1 & x & 0 & 0 \\ -1 & 0 & x & 0 \\ -1 & 0 & 0 & x \end{vmatrix}$$

$$= (x-3)\,x^4(x+3)$$

$$\mathrm{Spec}\,K_{3,3} = \begin{pmatrix} 3 & 0 & -3 \\ 1 & 4 & 1 \end{pmatrix}.$$

（ウ）　完全 2 部グラフ $K_{3,2}$ の隣接行列 A は，

$$\begin{pmatrix} 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 \end{pmatrix}$$

としてよい．よって，

$$\det(xI-A) = \begin{vmatrix} x & 0 & 0 & -1 & -1 \\ 0 & x & 0 & -1 & -1 \\ 0 & 0 & x & -1 & -1 \\ -1 & -1 & -1 & x & 0 \\ -1 & -1 & -1 & 0 & x \end{vmatrix}$$

$$= \begin{vmatrix} x & 0 & 0 & -1 & -1 \\ -x & x & 0 & 0 & 0 \\ -x & 0 & x & 0 & 0 \\ -1 & -1 & -1 & x & 0 \\ -1 & -1 & -1 & 0 & x \end{vmatrix}$$

$$= \begin{vmatrix} 0 & 0 & 0 & 0 & -1 \\ -x & x & 0 & 0 & 0 \\ -x & 0 & x & 0 & 0 \\ -1 & -1 & -1 & x & 0 \\ x^2-1 & -1 & -1 & -x & x \end{vmatrix} = \cdots$$

$$= x^3(x^2-6),$$

$$\mathrm{Spec}\, K_{3,2} = \begin{pmatrix} \sqrt{6} & 0 & -\sqrt{6} \\ 1 & 3 & 1 \end{pmatrix}.$$

定　理｜5.3.3

$\Gamma = (V, E)$ を n 頂点からなる k-正則グラフとし，$V = \{v_1, v_2, \cdots, v_n\}$ とする．このとき，次のことが成り立つ．

（1） k は Γ の固有値で，Γ が連結のとき k の重複度は 1．

（2） Γ の任意の固有値 λ に対し，$|\lambda| \leqq k$ である．

証 明

（1） Γ の隣接行列 A に対し，

$$A\,{}^t(1,1,\cdots,1)=k\,{}^t(1,1,\cdots,1)$$

となるので，k は Γ の固有値である．また，

$$A\,{}^t(x_1,x_2,\cdots,x_n)=k\,{}^t(x_1,x_2,\cdots,x_n)$$

として，x_j を $x_1,x_2,\cdots,x_n$ のうちで絶対値が最大なものとする(j を固定)．このとき，

$$\sum{}' x_i=kx_j$$

である．ただし $\sum{}'$ は，v_j と隣接な頂点 v_i を表す i についての和とする．いま，

$$\sum{}' x_i=x_{i_1}+x_{i_2}+\cdots+x_{i_k}$$

とすると，各 x_{i_l} の絶対値 $|x_{i_l}|$ は $|x_j|$ 以下なので，

$$x_{i_1}=x_{i_2}=\cdots=x_{i_k}=x_j$$

でなくてはならない．もし Γ が連結とすると，上の議論をくり返すことにより

$$x_1=x_2=\cdots=x_j=\cdots=x_n$$

を得る．

（2） Γ の隣接行列 A に対し，

$$A\,{}^t(x_1,x_2,\cdots,x_n)=\lambda\,{}^t(x_1,x_2,\cdots,x_n)$$

$${}^t(x_1,x_2,\cdots,x_n)\neq\mathbf{0}\qquad(\text{零ベクトル})$$

とすると，(1)と同様な議論によって(絶対値が最大な x_j に対して)，

$$\sum{}' x_i=\lambda x_j$$

を得る．したがって，

$$|\lambda|\,|x_j|=\left|\sum{}' x_i\right|\leqq\sum{}'|x_i|\leqq k|x_j|$$

が成り立ち，$|\lambda|\leqq k$ を得る．

定 理 | 5.3.4

$\Gamma=(V,E)$ を n 頂点からなるグラフとし，$V=\{v_1,v_2,\cdots,v_n\}$ とする．A を Γ の隣接行列，π を V 上の置換とすると，

$$\pi \in \mathrm{Aut}(\Gamma) \Longleftrightarrow P_\pi A = AP_\pi$$

証　明

$$P_\pi = (p_{ij}), \qquad A = (a_{ij})$$

とおく．いま，

$$v_h = (v_i)\pi, \qquad v_k = (v_j)\pi \tag{$*$}$$

として，$P_\pi A$ と AP_π の (i, k) 成分を求めると，

$$P_\pi A \text{ の } (i,k) \text{ 成分} = \sum_{l=1}^{n} p_{il}a_{lk} = a_{hk},$$

$$AP_\pi \text{ の } (i,k) \text{ 成分} = \sum_{l=1}^{n} a_{il}p_{lk} = a_{ij}$$

を得る．よって，

$P_\pi A = AP_\pi \Longleftrightarrow$ [(＊)をみたすすべての組に対して，v_h と v_k が隣接であるための必要十分条件は v_i と v_j が隣接であること．]

$\Longleftrightarrow \pi \in \mathrm{Aut}(\Gamma)$

が成り立つ．

定　理 | 5.3.5

グラフ Γ に対し，λ を重複度 1 の固有値とし，$\boldsymbol{x}\ (\neq \boldsymbol{0})$ をそれに対する実固有ベクトルとする．このとき，Γ のすべての自己同型写像 π に対し，$P_\pi \boldsymbol{x} = \pm \boldsymbol{x}$ が成り立つ．

証　明

定理 5.3.4 を使って，

$$A(P_\pi \boldsymbol{x}) = (AP_\pi)\boldsymbol{x} = P_\pi(A\boldsymbol{x}) = P_\pi(\lambda \boldsymbol{x}) = \lambda(P_\pi \boldsymbol{x}).$$

λ の重複度は 1 なので，

$$P_\pi \boldsymbol{x} = r\boldsymbol{x}$$

となる実数 r がある．V 上の置換としての π の位数を m とすれば，

$$r^m \boldsymbol{x} = (P_\pi)^m \boldsymbol{x} = I\boldsymbol{x} = \boldsymbol{x}.$$

よって，r は1または -1 でなくてはならない．

定　理 | 5.3.6

グラフ Γ が，位数が2より大きい自己同型写像をもつならば，Γ のある固有値の重複度は1より大きい．

証　明

Γ のすべての固有値の重複度は1とする．π を Γ の任意の自己同型写像とし，$\boldsymbol{x}(\neq \boldsymbol{0})$ を Γ の任意の実固有ベクトルとすると，定理5.3.5より

$$(P_\pi)^2 \boldsymbol{x} = \boldsymbol{x}$$

が成り立つ．ところが，$\boldsymbol{R}^n$ は Γ の実固有ベクトル全体によって生成されるので（n：Γ の位数），$(P_\pi)^2 = I$（単位行列）を得る．

定　理 | 5.3.7

$\Gamma = (V, E)$ を k-正則な頂点可移グラフとし，$V = \{v_1, v_2, \cdots, v_n\}$ とする．λ は Γ の重複度1の固有値とすると，以下が成り立つ．

（1）　n が奇数のとき $\lambda = k$.

（2）　n が偶数のとき $\lambda = 2t-k$．ここで，t は0以上 k 以下のある整数である．

証　明

$$\boldsymbol{x} = {}^t(x_1, x_2, \cdots, x_n) \neq \boldsymbol{0}$$

を λ に対する実固有ベクトルとし，π を Γ の任意の自己同型写像とすると，定理5.3.5より

$$P_\pi \boldsymbol{x} = \pm \boldsymbol{x}$$

である．Γ は頂点可移グラフであるから，各 $i = 2, 3, \cdots, n$ に対し，

$$(v_1)\pi_i = v_i$$

となる自己同型写像 π_i が存在する．置換行列 P_{π_i} の $(1, i)$ 成分は1なので，

$$x_i = \pm x_1 \qquad (i = 2, 3, \cdots, n) \tag{$*$}$$

を得る．

（1） もし $\lambda \neq k$ とすると，λ と k は実対称行列 A の異なる固有値なので，それらに対する固有ベクトルどうしは直交する．したがって，$\boldsymbol{x}$ と n 次元ベクトル ${}^t(1, 1, \cdots, 1)$ は直交するので，

$$\sum_{i=1}^{n} x_i = 0$$

となる．n は奇数なので，これは(＊)に反して矛盾である．

（2） (＊)から，v_1 と隣接な k 個の頂点 v_i に対応する i のうちで，t 個が $x_i = x_1$ であるとし，$k-t$ 個が $x_i = -x_1$ であるとする．そして，

$$A\boldsymbol{x} = \lambda\boldsymbol{x}$$

の第1成分に注目すると，

$$tx_1 - (k-t)x_1 = \lambda x_1$$

が成り立つ．よって，$\lambda = 2t-k$ を得る．

5.4 距離正則グラフ

本節では，対象とするグラフは連結な有限グラフに限るものとする．グラフ $\Gamma = (V, E)$ が**距離可移グラフ**であるとは，次の条件をみたすときにいう：V の元 u, v, x, y に対して

$$d(u, v) = d(x, y)$$

が成り立つならば，

$$(u)\sigma = x, \qquad (v)\sigma = y$$

となる Γ の自己同型写像 σ が存在する．

グラフ $\Gamma = (V, E)$ の直径を d とし，$i = 1, 2, \cdots, d$ に対し

$$\Delta_i = \{\{u, v\} \in V^{(2)} \mid d(u, v) = i\}$$

とおけば，グラフ Γ が距離可移のとき $(V, \{\Delta_i \mid 1 \leqq i \leqq d\})$ はクラス d のアソシエーションスキームとなる．また，直径 d のグラフ Γ に距離可移性を仮定しなくとも，$(V, \{\Delta_i \mid 1 \leqq i \leqq d\})$ がアソシエーションスキームになることは考えられる．そのようなグラフを，一般に**距離正則グラフ**という．近年，距

離正則グラフの研究の発展には目覚ましいものがある([洋；7] 参照).

なお，距離正則グラフであっても距離可移グラフではない例は，古くからいろいろと知られている(最初の発見は[論；1]).

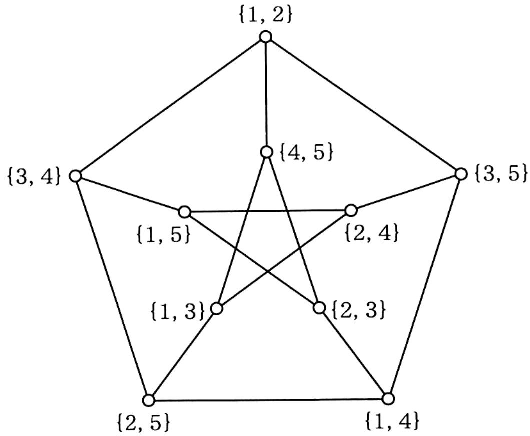
$(V, \{\Delta_i | 1 \leqq i \leqq d\})$ がアソシエーションスキームになる距離正則グラフ $\Gamma = (V, E)$ において，関係 Δ_1 に対する隣接行列 A_1 は(4.5節参照)，本節では隣接行列 A のことである．また，隣接行列 $A_1 = A$ に対応する $d+1$ 次の交叉行列 P_1 を(4.5節参照)，本節では B で表すことにする．そして B を，単に距離正則グラフ Γ の**交叉行列**ということにする．

例 5.4.1

(ア) ペテルセングラフ(例5.1.5)は距離可移グラフである．実際，

$$\Omega = \{1, 2, 3, 4, 5\}, \qquad \Gamma = (V, E), \qquad V = \Omega^{(2)},$$
$$E = \{\{u, v\} | u, v \in V,\ u \cap v = \emptyset\}$$

とおいたグラフはペテルセングラフになる．



そして，Ω 上の任意の置換は Γ の自己同型写像を引き起こす(実際，$\mathrm{Aut}(\Gamma) = S^{\Omega}$)．よって，$\Gamma$ は頂点可移グラフである．また，V の元 $\{\alpha_1, \alpha_2\}$ と $\{\beta_1, \beta_2\}$，および $\{\gamma_1, \gamma_2\}$ と $\{\delta_1, \delta_2\}$ が隣接とすると，

$$\{\alpha_1, \alpha_2\} \cap \{\beta_1, \beta_2\} = \{\gamma_1, \gamma_2\} \cap \{\delta_1, \delta_2\} = \emptyset.$$

そこで，

$$\{\alpha_1, \alpha_2\}^\sigma = \{\gamma_1, \gamma_2\}, \qquad \{\beta_1, \beta_2\}^\sigma = \{\delta_1, \delta_2\}$$

となる $\sigma \in \mathrm{Aut}(\Gamma)$ が存在する．さらに，V の元 $\{\alpha_1, \alpha_2\}$ と $\{\beta_1, \beta_2\}$，および $\{\gamma_1, \gamma_2\}$ と $\{\delta_1, \delta_2\}$ の距離が 2 とすると，

$$|\{\alpha_1, \alpha_2\} \cap \{\beta_1, \beta_2\}| = |\{\gamma_1, \gamma_2\} \cap \{\delta_1, \delta_2\}| = 1.$$

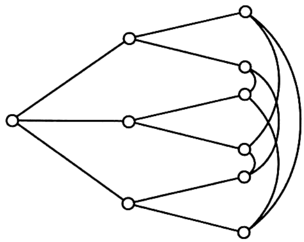
そこで，

$$\{\alpha_1, \alpha_2\}^\tau = \{\gamma_1, \gamma_2\}, \qquad \{\beta_1, \beta_2\}^\tau = \{\delta_1, \delta_2\}$$

となる $\tau \in \mathrm{Aut}(\Gamma)$ も存在する．したがって，Γ は距離可移グラフとなる．そして，Γ の交叉行列 B は次のようになる．

$$B = \begin{pmatrix} 0 & 1 & 0 \\ 3 & 0 & 1 \\ 0 & 2 & 2 \end{pmatrix}$$

なお，上記の交叉行列をもつ距離正則グラフがペテルセングラフと同型になることは，内周長が5になることに注目してやさしく確かめられる(下図参照)．



（イ） n, e を $2e \leqq n$ をみたす自然数とする．このとき，Ω を n 個の元からなる集合として，

$$V = \Omega^{(e)}, \qquad E = \{\{u, v\} \mid u, v \in V,\ |u \cap v| = e-1\}$$

によって定められるグラフ $\Gamma = (V, E)$ を**ジョンソングラフ** $J(n, e)$ という．$J(n, e)$ は距離可移グラフであるが，その説明は本質的に例 4.5.1(ア)と同じである．そして，Γ の交叉行列 B は次のようになる．

$$B=\begin{pmatrix} 0 & 1^2 & & & & O \\ e(n-e) & n-2 & \ddots & & & \\ & \ddots & \ddots & i^2 & & \\ & & \ddots & i(n-2i) & & \\ & & & (e-i)(n-e-i) & \ddots & \\ & & & & \ddots & e^2 \\ O & & & & n-2e+1 & e(n-2e) \end{pmatrix}$$

なお[論；27,35]などによって，上記の交叉行列をもつ距離正則グラフとしてジョンソングラフは特徴付けられている．

(ウ) d, q を自然数とし，$q \geqq 2$ とする．このとき，X を q 個の元からなる集合として，

$$V=\{(x_1, x_2, \cdots, x_d) \mid x_i \in X\},$$

$$E=\{\{u, v\} \mid u=(a_1, \cdots, a_d),\ v=(b_1, \cdots, b_d) \in V,\ a_i \neq b_i \text{ となる } i \text{ は } 1 \text{ つだけ}\}$$

によって定められるグラフ $\Gamma=(V, E)$ を**ハミンググラフ** $H(d, q)$ という．$H(d, q)$ も距離可移グラフであるが，その証明は本質的に例 4.5.1(イ)と同じである．そして，Γ の交叉行列 B は次のようになる．

$$B=\begin{pmatrix} 0 & 1 & & & & O \\ d(q-1) & q-2 & \ddots & & & \\ & (d-1)(q-1) & \ddots & \ddots & & \\ & & \ddots & \ddots & d-1 & \\ & & & \ddots & (d-1)(q-2) & d \\ O & & & & (q-1) & d(q-2) \end{pmatrix}$$

なお [論；10] によって，上記の交叉行列をもつ距離正則グラフとしてハミンググラフは特徴付けられている．

上の例を見ても分かるように，直径 d の距離正則グラフの交叉行列 B は，一般に次のような $d+1$ 次行列として表される(4.5 節参照)．

$$B = \begin{pmatrix} a_0 & c_1 & & & O \\ b_0 & a_1 & \ddots & & \\ & b_1 & \ddots & & \\ & & \ddots & a_{d-1} & c_d \\ O & & & b_{d-1} & a_d \end{pmatrix}$$

$$a_i = p^i_{1,i}, \quad b_i = p^i_{1,i+1}, \quad c_i = p^i_{1,i-1}.$$

定　理 | 5. 4. 2

直径が d の距離正則グラフ Γ は，ちょうど $d+1$ 個の相異なる固有値をもつ．とくに，Γ の交叉行列 B の固有値はすべて異なる．

証　明

定理 5. 3. 1 より，Γ は $d+1$ 個以上の相異なる固有値をもつ．一方，4. 5 節で述べた説明により，A の相異なる固有値の集合は，$d+1$ 次行列 B のそれと一致する．

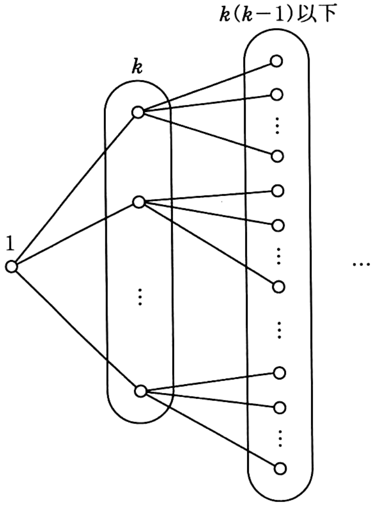
定理 5. 4. 2 により，距離正則グラフ Γ の任意の固有値 θ の重複度は，定理 4. 5. 3 を用いて原理的に求めることができる．

さて，$\Gamma=(V,E)$ を直径が d の k-正則グラフとし ($k \geqq 2$)，$|V|=n$ とすると，

$$n \leqq 1+k+k(k-1)+\cdots+k(k-1)^{d-1}$$

が成り立つ(右図参照)．

上の不等式で等号が成立するとき，Γ を**ムアーグラフ**という．本節の後半ではそれについて述べるが，距離正則グラフの研究が発展したきっかけには，ムアーグラフについての研究があったからだと言えるだろう．



定　理 | 5.4.3

$\Gamma=(V,E)$ を直径が d のグラフとする．u,v を $d(u,v)=i\ (0\leqq i\leqq d)$ となる頂点とするとき，

$$a_i=|\{x\in V\,|\,d(x,u)=1,\ \ d(x,v)=i\}|\quad (i=0,1,\cdots,d),$$
$$b_i=|\{x\in V\,|\,d(x,u)=1,\ \ d(x,v)=i+1\}|\quad (i=0,1,\cdots,d-1),$$
$$c_i=|\{x\in V\,|\,d(x,u)=1,\ \ d(x,v)=i-1\}|\quad (i=1,2,\cdots,d)$$

がいずれも u,v のとり方によらず i のみによって定まるならば，Γ は距離正則グラフである．

証　明

最初に b_0 に注目することにより，Γ は b_0-正則であることが分かる．以後，b_0 を k で表す．

次に，$V=\{v_1,v_2,\cdots,v_n\}$ とし，各 $i\ (0\leqq i\leqq d)$ に対し，距離 i の関係を表す行列 A_i を次のように定める．A_i は n 次正方行列で，

$$A_i \text{ の } (s,t) \text{ 成分} = \begin{cases} 1 & (d(v_s,v_t)=i) \\ 0 & (d(v_s,v_t)\neq i). \end{cases}$$

とくに，$A_1 = A$ (Γ の隣接行列)，$A_0 = I$ (単位行列)である．

$$A_{d+1} = A_{-1} = O \qquad (\text{零行列}), \qquad c_{d+1} = b_{-1} = 0$$

とおくと，仮定より

$$A_1 A_r = c_{r+1} A_{r+1} + a_r A_r + b_{r-1} A_{r-1}$$

が $r = 0, 1, \cdots, d$ に対して成り立つ．ここで $c_{r+1} \neq 0$ ($r = 1, 2, \cdots, d-1$) に留意すると，各 $r = 1, 2, \cdots, d-1$ に対して，A_{r+1} は $A_1 = A$ の $r+1$ 次多項式として表されることが分かる．したがって，$M(n, \boldsymbol{R})$ の部分環

$$S = \{f(A) \mid f(x) \in \boldsymbol{R}[X]\}$$

に，$A_1 = A, A_2, \cdots, A_d$ はすべて含まれる．いま，行列 J をすべての成分が1の n 次行列とすると，

$$J = I + A_1 + A_2 + \cdots + A_d,$$
$$(A - kI)J = AJ - kJ = O$$

となることから，A の最小多項式の次数は $d+1$ である．したがって，S を $\boldsymbol{R}$ 上の線形空間とみたときの次元は $d+1$ である．それゆえ，$\{I, A, A^2, \cdots, A^d\}$ も $\{A_0 = I, A_1 = A, A_2, \cdots, A_d\}$ も線形空間 S の基底となる．とくに，任意の i, j ($0 \leqq i, j \leqq d$) に対し，

$$A_i A_j = \sum_{h=0}^{d} \mu_{ij}^h A_h$$

となる i, j, h のみによって定まる定数 μ_{ij}^h ($h = 0, 1, \cdots, d$) がある．これは，グラフ Γ が距離正則であることを意味している．

定　理 | 5. 4. 4

直径が d の k-正則グラフ $\Gamma = (V, E)$ がムアーグラフとなるならば ($k \geqq 2$)，Γ は交叉行列 B が次の形をした距離正則グラフとなる．

$$B = \begin{pmatrix} 0 & 1 & & & O \\ k & 0 & \ddots & & \\ & k-1 & \ddots & & \\ & & \ddots & 0 & 1 \\ O & & & k-1 & k-1 \end{pmatrix}$$

証　明

Γ の内周長が $2d+1$ になることに注目して，定理 5.4.3 を用いればよい．

定　理 | 5.4.5

直径が 2 の k-正則グラフ $\Gamma=(V,E)$ が，ムアーグラフとなるならば ($k\geqq 2$)，$k=2,3,7$ または 57 である．

証　明

$|V|=n$，A を Γ の隣接行列，J をすべての成分が 1 の n 次行列とすると，定理 5.4.4 の結論と定理 5.4.3 の証明から，

$$A^2=k\cdot I+0\cdot A+1\cdot(J-A-I),$$
$$A^2+A-(k-1)I=J$$

を得る．定理 5.3.3 より，k は A の固有値で重複度は 1．また，その固有ベクトル ${}^t(1,1,\cdots,1)$ に対する J の固有値は n で，J は他に固有値 0 を重複度 $n-1$ でもつ．

いま，λ を k と異なる A の固有値とすると，

$$\lambda^2+\lambda-(k-1)=0,$$
$$\lambda=\frac{-1\pm\sqrt{4k-3}}{2}$$

が成り立つ．そこで，

$$\mathrm{Spec}\,\Gamma=\begin{pmatrix} k & \dfrac{-1+\sqrt{4k-3}}{2} & \dfrac{-1-\sqrt{4k-3}}{2} \\ 1 & l & m \end{pmatrix}$$

とおくと，

$$1+l+m=n=1+k+k(k-1)=1+k^2,$$
$$l+m=k^2$$

を得る．また，A の固有和を考えると，

$$k+\frac{l}{2}(-1+\sqrt{4k-3})+\frac{m}{2}(-1-\sqrt{4k-3})=0,$$

$$2k-(l+m)+\sqrt{4k-3}(l-m)=0,$$
$$k^2-2k=\sqrt{4k-3}(l-m)$$

を得る．ここで $\sqrt{4k-3}=r$ とおくと，

$$k^2-2k=r(l-m) \tag{$*$}$$

となる．

したがって，もし r が無理数ならば，

$$k^2-2k=0, \qquad k=2$$

でなくてはならない．また，もし r が有理数ならば，

$$4k-3=r^2$$

から，r は整数になる．そして，

$$k=\frac{r^2+3}{4}$$

を(＊)に代入することにより，

$$\left(\frac{r^2+3}{4}\right)^2-2\left(\frac{r^2+3}{4}\right)=r(l-m)=r(2l-k^2)$$
$$=r\left(2l-\left(\frac{r^2+3}{4}\right)^2\right),$$
$$r^5+r^4+6r^3-2r^2+9r-32rl-15=0$$

を得る．よって r は 15 の約数となり，$r=1,3,5,15$ に応じて，$k=1,3,7,57$ となる．

上の定理において，$k=2$ に対応するグラフは長さ 5 のサイクルであり，$k=3$ に対応するグラフはペテルセングラフであり，$k=7$ に対応するグラフは**ホフマン-シングルトングラフ**とよばれる距離可移グラフである([論；17] 参照)．なお，$k=57$ に対応するグラフの存在性は未解決であるが，存在すれば頂点可移グラフではないことが知られている([洋；8] 参照)．

本節の最後に，次の定理を紹介する．

定理 | 5.4.6 ……Hoffman-Singleton [論；17], Bannai-Ito [論；2], Damerell [論；8]

直径 d が 3 以上の k-正則グラフ Γ がムアーグラフとなるならば ($k\geqq 2$), $k=2$ に限る．すなわち，Γ は長さ $2d+1$ のサイクルである．

Appendix

無限次数多重可移置換群

無限次数の置換群は，群論ばかりでなく位相数学，数学基礎論などの立場からも研究されているが，ここでは定理 2.2.5 (Jordan)のその後の発展について述べよう．

1872 年に証明された Jordan の定理は，4 点の固定部分群が単位群になる有限次数 4 重可移置換群の分類であった．その 80 年後の 1952 年に，Tits はそれにおける有限次数の条件を除いても同じ結論が成り立つことを証明した([論；36] 参照)．そして 1954 年には，Hall によって次のように拡張された．

定　理 | A. 1 ……………………………………………………………Hall[**論；15**]

Ω を有限または無限集合とする．G は Ω 上の 4 重可移置換群で，Ω の相異なる 4 つの元の $\alpha, \beta, \gamma, \delta$ に対して $G_{\alpha\beta\gamma\delta}$ は奇数位数とする．このとき，G は S_4, S_5, A_6, A_7 または M_{11} のどれかと一致する．

定理 6.1 の結果をふまえると，4 点の固定部分群が有限群になる無限次数 4 重可移置換群の存在性に目が向くことは自然である．なお，定理 3.2.3 における体 K が無限体の場合を考えると，3 点の固定部分群が有限群になる無限次数 3 重可移置換群の存在性は明らかである．

1970 年代後半に，筆者は東京大学の榎本彦衛研究室での組合せ論および置換群論のセミナーに参加していたが，そこでの宮本泉氏からのアドバイスをきっかけに次の結果を 1978 年に得た．

定　理 | A. 2 ……………………………………………………Yoshizawa[**論；37**]

G を無限集合 Ω 上の 4 重可移置換群とすると，Ω の相異なる 4 つの元 $\alpha, \beta, \gamma, \delta$ に対して $G_{\alpha\beta\gamma\delta}$ は無限群である．

上定理の証明は，群論の基本的な性質だけを用いて短く完成したので，以下それを解説する．最初に準備として，次の定理を証明する．

定理 | A. 3

p を素数，t を p 以上の整数とし，G を以下の条件をみたす無限集合 Ω 上の置換群とする：Ω の相異なる任意の t 個の元 $\alpha_1, \alpha_2, \cdots, \alpha_t$ に対し，$|G_{\alpha_1\alpha_2\cdots\alpha_t}|$ は有限で p の倍数．このとき，G は Ω の無限個の元を固定する位数 p の元をもつ．

証明

G のすべての位数 p の元 g は $|I(g)| < \infty$ をみたすとして，矛盾を導くことにする．$\alpha_1, \alpha_2, \cdots, \alpha_t$ を Ω の相異なる t 個の元とし，x を $G_{\alpha_1\alpha_2\cdots\alpha_t}$ の位数 p の元とする（シローの定理を参照）．$I(x)$ は有限集合であるから，

$$|I(x)| = s, \qquad I(x) = \{\alpha_1, \alpha_2, \cdots, \alpha_t, \cdots, \alpha_s\}$$

とおく．いま x は，互いに共通な文字をもたないいくつかの長さ p の巡回置換の合成として表されるので（例 1. 2. 7 参照），$(\beta_1, \beta_2, \cdots, \beta_p)$ をその 1 つの長さ p の巡回置換とする．明らかに，x は正規化群 $N_G(G_{\beta_1\beta_2\cdots\beta_p\alpha_1\cdots\alpha_{t-p}})$ の元である．そして，有限群 $H = G_{\beta_1\beta_2\cdots\beta_p\alpha_1\cdots\alpha_{t-p}}$ の各元 h を $g^{-1}hg$ に移す写像は，H の自己同型写像 φ を引き起こしている．とくに φ は，H のシロー p-部分群全体からなる集合の上に作用している．ところがシローの定理により，H のシロー p-部分群の個数は p で割ると 1 余る数である．それゆえ，H のあるシロー p-部分群 $P\,(\neq 1)$ に対し，

$$x^{-1}Px = P$$

でなくてはならない．よって，写像 φ は P における位数 p の元全体からなる集合の上に作用している．

ところが再びシローの定理により，P の位数 p の元の個数は p で割ると 1 余る数である．したがって，P のある位数 p の元 y に対し，

$$x^{-1}yx = y$$

でなくてはならない．すなわち x と y は可換となり，それゆえ

$$(I(x))y = I(x) = \{\alpha_1, \alpha_2, \cdots \alpha_t, \cdots, \alpha_s\}$$

が成り立つ．

以上から，x の巡回置換分解における任意の長さ p の巡回置換 $(\gamma_1, \gamma_2, \cdots, \gamma_p)$ に対し，$\gamma_1, \gamma_2, \cdots, \gamma_p$ をすべて固定する $G_{(I(x))}$ の位数 p の元 y が存在する．ただし $G_{(I(x))}$ は，G における $I(x)$ の集合としての固定部分群である（2.2 節参照）．

ここで背理法の仮定から，x に対して上記の $(\gamma_1, \gamma_2, \cdots, \gamma_p)$ は無限個存在し，そしてさらに $G_{(I(x))}$ の位数 p の元は無限個存在することが分かる．よって

$$|G_{(I(x))}| = \infty$$

となるが，それは等式

$$|G_{(I(x))}| = |(G_{(I(x))})^{I(x)}| \cdot |G_{I(x)}|$$

の右辺の積が有限であることに反する．

定理 A. 2 の証明

無限集合 Ω 上の 4 重可移置換群 G があって，Ω の相異なる 4 つの元 $\alpha, \beta, \gamma, \delta$ に対して $G_{\alpha\beta\gamma\delta}$ は有限群であるとする．これから矛盾を導くことによって定理を証明する．

いま，P を $G_{\alpha\beta\gamma\delta}$ のシロー 2-部分群とすると，定理 A. 1 より $P \neq 1$ である．シローの定理と定理 2. 2. 4 により，$N_G(P)^{I(P)}$ は $I(P)$ 上の 4 重可移置換群である．さらに $N_G(P)^{I(P)}$ の 4 点の固定部分群は奇数位数の群である．それゆえ再び定理 A. 1 を用いて，$N_G(P)^{I(P)}$ は S_4, S_5, A_6, A_7 または M_{11} のどれかと置換群として同型になる．とくに，$|I(P)| < \infty$ である．

ここで $p = 2$，$t = 4$ として定理 A. 3 を適用すると，G は $|I(x)| = \infty$ となる位数 2 の元 x をもつことが分かる．Q_0 を $G_{I(x)}$ のシロー 2-部分群とし，$\alpha_1, \alpha_2, \alpha_3, \alpha_4$ を $I(Q_0)$ の相異なる任意の 4 つの元とすると，シローの定理により $P_0 \supseteqq Q_0$ をみたす $G_{\alpha_1\alpha_2\alpha_3\alpha_4}$ のシロー 2-部分群 P_0 が存在する．

G の 4 重可移性とシローの定理から，$|I(P_0)| = |I(P)|$ がいえるので，

$$|I(P_0)| < \infty, \quad |I(Q_0)| = \infty$$

が分かる．よって，定理 1. 7. 1 により $N_{P_0}(Q_0) \supsetneqq Q_0$ が成り立つ．ところが Q_0

は $G_{I(Q_0)}$ のシロー 2-部分群であるので，$I(N_{P_0}(Q_0)) \subsetneqq I(Q_0)$ でなくてはならない．したがって，

$$(N_G(Q_0)^{I(Q_0)})_{\alpha_1\alpha_2\alpha_3\alpha_4} = (N_G(Q_0)_{\alpha_1\alpha_2\alpha_3\alpha_4})^{I(Q_0)}$$

は偶数位数の置換群になる．

今度は定理 A. 3 を $N_G(Q_0)^{I(Q_0)}$ に適用すると，$N_G(Q_0)^{I(Q_0)}$ は $|I(x_0)| = \infty$ となる位数 2 の元 x_0 をもつことが分かる．そして Q_1 を $G_{I(x_0)}$ の 1 つのシロー 2-部分群とすれば，明らかに

$$|P| > |Q_1| > |Q_0|$$

が成り立つ．次に，Q_0 に対して行った議論を Q_1 に対して適用すれば，$N_G(Q_1)^{I(Q_1)}$ は $|I(x_1)| = \infty$ となる位数 2 の元 x_1 をもつことが分かる．そして Q_2 を $G_{I(x_1)}$ の 1 つのシロー 2-部分群とすれば，明らかに

$$|P| > |Q_2| > |Q_1| > |Q_0|$$

が成り立つ．

上の議論をくり返すことにより，G は

$$|P| > \cdots > |Q_n| > |Q_{n-1}| > \cdots > |Q_1| > |Q_0|$$

をみたす 2-部分群 $Q_0, Q_1, \cdots, Q_{n-1}, Q_n, \cdots$ の無限列をもつことになる．これは，P が有限群であることに反する．

最後に，多重可移性より条件が弱いある性質について簡単に触れておこう．

実数体 $\boldsymbol{R}$ から $\boldsymbol{R}$ の上への 1 対 1 の連続写像 f で，

$$f(a) < f(b) \Longleftrightarrow a < b \qquad (a, b \in \boldsymbol{R})$$

をみたすもの全体からなる集合 G を考える．t を任意に固定した自然数とし，

$$\alpha_1 < \alpha_2 < \cdots < \alpha_t, \qquad \beta_1 < \beta_2 < \cdots < \beta_t$$

をみたす $\boldsymbol{R}^{(t)}$ の任意の元 $\{\alpha_1, \alpha_2, \cdots, \alpha_t\}$，$\{\beta_1, \beta_2, \cdots, \beta_t\}$ をとると，

$$(\{\alpha_1, \alpha_2, \cdots, \alpha_t\})g = \{\beta_1, \beta_2, \cdots, \beta_t\}$$

となる $g \in G$ は必ず存在する．すなわち，$\boldsymbol{R}$ 上の置換群である G は $\boldsymbol{R}^{(t)}$ 上可移に作用している．しかしながら，明らかに G は $\boldsymbol{R}$ 上 2 重可移には作用していない．

上記の例を見るまでもなく，無限集合 Ω 上の置換群 G が，Ω 上 t 重可移に

作用することと $\Omega^{(t)}$ 上可移に作用することの両者の間には，大きな違いがあると考えるのが自然であろう．ところが Ω が有限集合の場合は，有限単純群の分類が完成する以前から両者の間には大きな違いのないことが分かっていた([論；20, 23] 参照)．

無限集合 Ω 上の置換群 G に**局所有限**，すなわち有限個の元で生成される部分群は有限群，という条件が加わると，t 重可移性がなくても，$\Omega^{(t)}$ 上に可移 ($t \geqq 9$) という条件が付くことによって，定理 A. 2 と同様な結果(t 点の固定部分群は無限群)が得られる([論；41] 参照)．

参考文献

和書

1 伊藤昇　復刊 有限群論（共立出版）2001年

2 榎本彦衛　グラフ学入門（日本評論社）1988年

3 榎本彦衛　情報数学入門（新曜社）1982年

4 大山豪　有限置換群（裳華房）1981年

5 齋藤正彦　線型代数入門（東京大学出版会）1995年

6 佐武一郎　線型代数学（裳華房）1974年

7 鈴木通夫　有限単純群（紀伊國屋書店）1987年

8 都筑俊郎　有限群と有限幾何（岩波書店）1976年

9 永尾汎　群とデザイン（岩波書店）1974年

10 永尾汎　代数学（朝倉書店）1983年

11 原田耕一郎　群の発見（岩波書店）2001年

12 松坂和夫　集合・位相入門（岩波書店）1989年

13 芳沢光雄　高校数学から理解して使える経営ビジネス数学（共立出版）2003 年

洋書

1 I. Anderson (1990), *Combinatorial designs* (Ellis Horwood).

2 E. Bannai and T. Ito (1984), *Algebraic Combinatorics* I (Benjamin).

3 T. Beth, D. Jungnickel and H. Lenz (1999), *Design Theory* vol. 1 (Cambridge).

4 T. Beth, D. Jungnickel and H. Lenz (1999), *Design Theory* vol. 2 (Cambridge).

5 N. Biggs (1971), *Finite Groups of Automorphisms* (Cambridge).

6 N. Biggs (1974), *Algebraic graph theory* (Cambridge).

7 A. E. Brouwer, A. M. Cohen and A. Neumaier (1989), *Distance-regular graphs* (Springer).

8 P. J. Cameron (1999), *Permutation Groups* (Cambridge).

9 P. J. Cameron, J. H. van Lint (1991), *Designs, Graphs, Code and their Links* (Cambridge).

10 C. J. Colbourn and M. J. Colbourn editors (1985), *Algorithms in combinatorial design theory* (North-Holland).

11 D. M. Cvetkovic, M. Doob and H. Sachs (1980), *Spectra of graphs* (Academic Press).

12 J. D. Dixon and B. Mortimer (1996), *Permutation Groups* (Springer).

13 C. D. Godsil (1993), *Algebraic Combinatorics* (Chapman & Hall).

14 M. Hall (1986), *Combinatorial theory* (Wiley).

15 D. S. Passman (1968), *Permutation Groups* (Benjamin).

16 H. Wielandt (1964), *Finite permutation groups* (Academic Press).

論文

1 G. M. Adel'son-Vel'skii, B. Ju. Veisfeiler, A. A. Leman and I. A. Faradzev (1969), Example of a graph without a transitive automorphism group. *Soviet Math. Dokl.* 10, 440-441.

2 E. Bannai and T. Ito (1973), On finite Moore graphs. *J. Fac. Sci. Univ. Tokyo,* Sect IA 20, 191-208.

3 A. Bochert (1889), Über die Zahl verschiedener Werte, die eine Funktion gegebener Buchstaben durch Vertauschung derselben erlangen kann. *Math. Ann.* 33, 584-590.

4 R. C. Bose and S. S. Shrikhande (1960), On the construction of sets of mutually orthogonal Latin squares and the falsity of a conjecture of Euler. *Trans. Amer. Math. Soc.* 95, 191-209.

5 R. C. Bose, S. S. Shrikhande and E. T. Parker (1960), Further results on the construction of mutually orthogonal Latin squares and the falsity of Euler's conjecture. *Canad. J. Math.* 12, 189-203.

6 I. Z. Bouwer (1972), On edge but not vertex transitive regular graphs. *J. Comb. Theory* (B) 12, 32-40.

7 A. Bremner (1979), A diophantine equation arising from tight 4-designs. *Osaka J. Math.* 16, 353-356.

8 R. M. Damerell (1973), On Moore graphs. *Proc. Cambridge Philos. Soc.* 74, 227-236.

9 R. H. F. Denniston (1976), Some new 5-designs. *Bull. London Math. Soc.* 8, 263-267.

10 Y. Egawa (1981), Characterization of $H(n, q)$ by the parameters. *J. Comb. Theory* (A) 31, 108-125.

11 H. Enomoto, N. Ito and R. Noda (1979), Tight 4-designs. *Osaka J. Math.* 16, 39-43.

12 R. Frucht (1949), Graphs of degree three with a given abstract group. *Canad. J. Math.* 1, 365-378.

13 C. D. Godsil (1978), GRR's for non-solvable groups. *Coll. Math. Soc. Janos Bolyai* 25, 221-239.

14 C. D. Godsil (1980), Neighbourhoods of transitive graphs and GRR's. *J. Comb. Theory* (B) 29, 116-140.

15 M. Hall (1954), On a theorem of Jordan. *Pacific J. Math.* 4, 219-226.

16 D. Hetzel (1976), Über regulare graphische Darstellung von auflosbaren Gruppen, Diplomarbeit, Technische Universitat Berlin.

17 A. J. Hoffman and R. R. Singleton (1960), On Moore graphs with diameters 2 and 3. *IBM J. Res. Develop.* 4, 497-504.

18 W. Imrich (1969), Graphs with transitive abelian automorphism group. *Coll. Math. Soc. Janos Bolyai* 4, 651-656.

19 C. Jordan (1873), Sur la limite de transitivite des groupes non-alternees. *Bull. Soc. Math. France* 1, 40-71.

20 W. M. Kantor (1972), k-homogeneous groups. *Math. Z.* 124, 261-265.

21 E. S. Kramer, S. S. Magliveras and R. Mathon (1989), The Steiner systems $S(2, 4, 25)$ with nontrivial automorphism group. *Discrete Math.* 77, 137-157.

22 I. Landgev and V. D. Tonchev (1989), Automorphisms of 2-(22,8,4) designs. *Discrete Math.* 77, 177-189.

23 D. Livingstone and A. Wagner (1965), Transitivity of finite permutation groups on unordered sets. *Math. Z.* 90, 393-403.

24 B. Marggraf (1892), Über primitive Gruppen mit transitiven Untergruppen geringeren Grades. Dissertation, Giessen.

25 W. I. Miller (1971), Even and odd permutations. *Mathematics Associations of Two-Year Colleges Journal* 5, 32.

26 W. H. Mills (1978), A new 5-designs. *Ars. Combinatoria* 6, 193-195.

27 A. Neumaier (1985), Characterization of a class of distance regular graphs. *J. reine*

angew. Math. 357, 182-192.

28 D. K. Ray-Chaudhuri and R. M. Wilson (1971), Solution of Kirkman's schoolgirl problem. *Symp. Pure Math.* 19, 187-203.

29 D. K. Ray-Chaudhuri and R. M. Wilson (1975), On t-designs. *Osaka J. Math.* 12, 737-744.

30 J. Seberry and M. Yamada (1992), Hadamard matrices, sequences, and block designs. *Contemporary design theory* (Wiley), 431-560.

31 C. C. Sims (1970), Computational methods in the study of permutation groups. *Computational Problems in Abstract Algebra* (Pergamon Press), 169-184.

32 G. Tarry (1900), Le probleme des 36 officiers. *C. R. Acad. Franc. pour l'Avanc. de Sci. Naturel* 1, 122-123; 2, 170-203.

33 L. Teirlinck (1987), Nontrivial t-designs without repeated blocks exist for all t. *Discrete Math.* 65, 301-311.

34 L. Teirlinck (1989), Locally trivial t-designs and t-designs without repeated blocks. *Discrete Math.* 77, 345-356.

35 P. Terwilliger (1986), The Johnson graph $J(d,r)$ is unique if $(d,r) \neq (2, 8)$. *Discrete Math.* 58, 175-189.

36 J. Tits (1952), Sur les groupes doublement transitifs continus. *Comment. Math. Helv.* 26, 203-224.

37 M. Yoshizawa (1979), On infinite four-transitive permutation groups. *J. London Math. Soc.* (2) 19, 437-438.

38 M. Yoshizawa (1981), On block-schematic Steiner systems $S(t, t+1, v)$. *Canad. J. Math.* 33, 1432-1438.

39 M. Yoshizawa (1989), Graphs with given group. *Osaka J. Math.* 26, 789-806.

40 M. Yoshizawa (1990), On block-schematic Steiner systems $S(t, t+2, v)$ and $S(t, t+3, v)$. *Hokkaido Math. J.* 19, 481-493.

41 M. Yoshizawa (2002), On locally finite k-homogeneous permutation groups. *Arch. Math.* 78, 1-4.

索引

数字・記号

15 ゲーム……52
2 部グラフ……127
2 面体群……126
G-軌道……30
p-群……28
t 重可移……45
Wedderburn の定理……39

あ行

アーベル群……5
アソシエーションスキーム……111
アダマール型のデザイン……98
アフィン平面……90
位数……8, 90, 98, 121
一般線形群……17, 65
イデアル……35
ウィットシステム……88
オイラー関数……24

か行

カークマンの女子学生問題……93
可移……45
可移拡大……70
可移拡大可能……70
外部自己同型群……23
可解……133
可換……5
可換環……34
可換群……5
可換体……34
核……19, 36
加法群……5
環……33
完全 2 部グラフ……127
完全グラフ……127
完全直交系……43
奇置換……8
軌道……30
軌道行列……110
基本可換群……33
逆元……5
逆写像……1
共役……15
共役類……15
局所有限……155
距離可移グラフ……142
距離正則グラフ……142
近傍……122
偶置換……8
クラス……111
グラフ……121
グラフ正則表現……133
群……5
ケイリーグラフ……129
結合行列……95
結合法則……5
原始置換群……47
交換法則……5

交叉行列 ……116, 143
交叉数 ……117
交代群 ……8
合同 ……vii
合同変換群 ……14
互換 ……3
固定点集合 ……50
固定部分群 ……13, 49
固有多項式 ……135
固有値 ……135
固有ベクトル ……135

さ行

サイクル ……123
最小多項式 ……135
サイズ ……121
四元数群 ……83
自己同型群 ……22, 54, 88, 122
自己同型写像 ……22, 88, 122
指数 ……13
次数 ……9, 122
自然な準同型写像 ……20
実数体 ……34
始点 ……123
自明な正規部分群 ……17
自明な部分群 ……9
射影一般線形群 ……65
射影幾何の基本定理 ……95
射影空間 ……67
射影直線 ……67
射影特殊線形群 ……65
射影平面 ……67, 90
斜体 ……34
集合としての固定部分群 ……49
終点 ……123
シュタイナーシステム ……88
巡回群 ……10
巡回置換 ……3
巡回置換分解 ……11
準同型写像 ……19, 36
準同型定理 ……20, 37
剰余環 ……35
剰余群 ……17
ジョンソングラフ ……144
ジョンソンスキーム ……112
シロー p-部分群 ……28
シローの定理 ……30
真部分群 ……9
スペクトラム ……135
整域 ……34
正規化群 ……16
正規部分群 ……17
生成 ……9, 38
生成系 ……10
生成元 ……10
正則 ……46, 126
正則グラフ ……126
接続 ……122
全射 ……1

全単射 ……1
像 ……19, 36
素体 ……38

た行

体 ……34
対称群 ……3
対称的 ……96
タイト ……104
多重可移 ……45
単位群 ……9
単位元 ……5, 34
単射 ……1
単純群 ……17
置換 ……1
置換行列 ……135
置換群 ……9
置換群として同型 ……20
中心 ……17
中心化群 ……16
頂点 ……121
頂点可移グラフ ……128
頂点集合 ……121
直積 ……25, 26
直線 ……67
直径 ……125
直交 ……41
デザイン ……87
点 ……vi, 67
同型 ……19, 20, 36, 87, 122
同型写像 ……19, 36, 87, 122
同型定理 ……21
特殊線形群 ……18, 65
特性部分群 ……23

な行

内周長 ……125
内部自己同型写像 ……23
長さ ……30, 123

は行

ハミンググラフ ……145
ハミングスキーム ……112
半正則 ……46
半直積 ……26
非原始系 ……48
非原始置換群 ……47
左イデアル ……35
左剰余類 ……12
左代表系 ……13
標数 ……38
非連結 ……124
フィッシャーの不等式 ……96
複素数体 ……34
部分環 ……36
部分空間 ……67
部分群 ……9
部分体 ……37
ブロック ……47
分解可能 ……92
分配法則 ……33

平面 ……67
平面グラフ ……126
平面的グラフ ……126
ペテルセングラフ ……125
辺 ……121
辺可移グラフ ……129
辺集合 ……121
ボーズ-メスナー多元環 ……116
補デザイン ……98
ホフマン-シングルトングラフ …150

ま行

マジックS10 ……57
マシュー群 ……70, 75, 76, 78
右イデアル ……35
右剰余類 ……13
右代表系 ……13
道 ……123
ムアーグラフ ……146
無限グラフ ……121
無限群 ……8
無向グラフ ……121

や行

有限グラフ ……121
有限群 ……8
有限体 ……39
有限的対称群 ……8
有向グラフ ……122
誘導デザイン ……88
有理数体 ……34
有理整数環 ……34

ら行

ラグランジュの定理 ……13
ラテン方陣 ……40
ラムゼー現象 ……124
ランク ……71
両側イデアル ……35
両側剰余類 ……71
両側分解 ……71
隣接 ……122
隣接行列 ……115, 134
類数 ……15
零元 ……5
レス積 ……113
連結 ……124
連結成分 ……124

わ行

和 ……5

芳沢光雄(よしざわ・みつお)
1953年　東京生まれ
1975年　学習院大学理学部数学科卒業
1983年　慶應義塾大学商学部助教授
1996年　城西大学理学部教授
2000年　東京理科大学理学部教授(大学院理学研究科教授)
専門は数学・数学教育　理学博士

著書
『高校「数学基礎」からの市民の数学』,
『子どもが算数・数学好きになる秘訣』(以上, 日本評論社),
『ビジネス数学入門』(日経文庫),
『高校数学から理解して使える経営ビジネス数学』(共立出版),
『ふしぎな数のおはなし』,『どうして?に挑戦する算数ドリル』(以上, 数研出版)
他多数

置換群(ちかんぐん)から学(まな)ぶ組合(くみあわ)せ構造(こうぞう)

発行日　2004年11月15日　第1版第1刷発行

著　者　芳沢光雄
発行者　林　克行
発行所　株式会社 日本評論社
〒170-8474
東京都豊島区南大塚3-12-4
電話　03-3987-8621(販売)
03-3987-8599(編集)
印　刷　株式会社 精興社
製　本　株式会社 精光堂
装　幀　清水良洋＋西澤幸恵(Push-up)

ISBN 4-535-78379-9 Printed in Japan